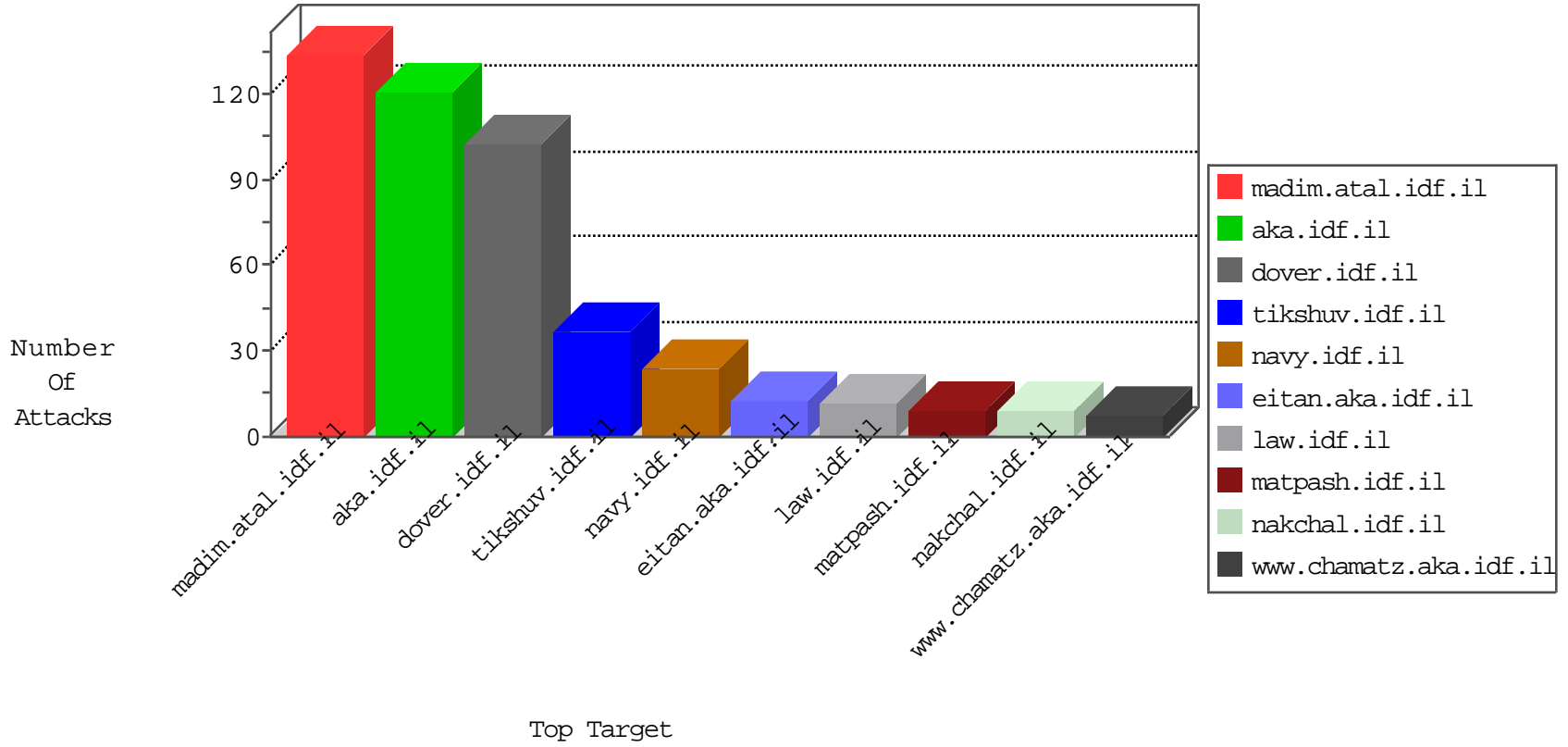


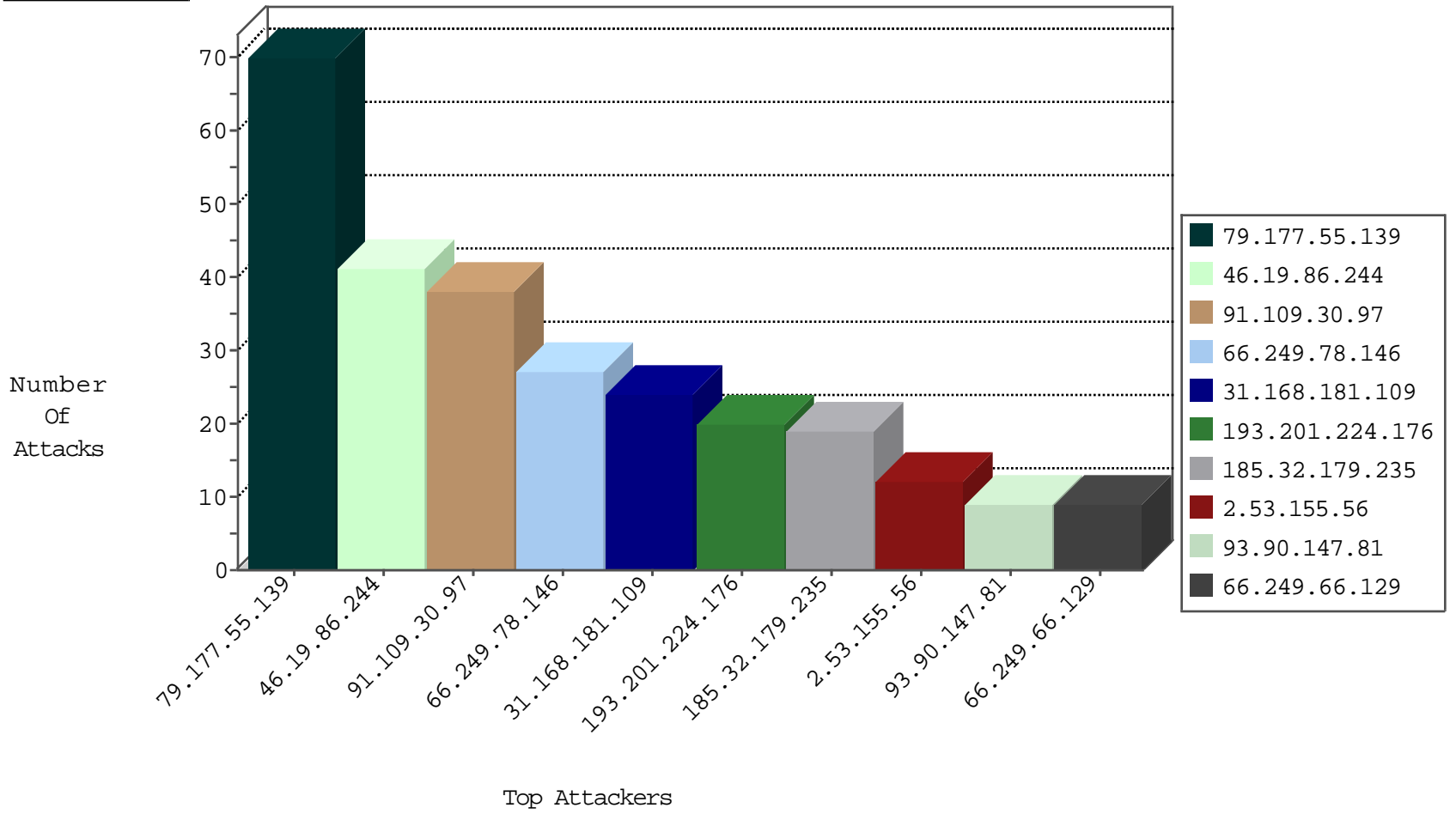
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
94.102.49.116	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
94.102.49.116	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.102.52.10	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
176.31.60.249	France	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.90.147.81	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.90.147.81	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
193.201.224.176	147.237.77.216	Ukraine	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1
185.34.0.141	147.237.77.233	Germany	atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.79.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
85.131.208.140	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
65.181.123.161	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
189.219.89.142	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.65.154.27	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
85.131.208.140	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.72.156	Germany	aman.idf.il	ET SCAN Potential SSH Scan	1
65.181.123.161	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.121	United States	e.navy.idf.il	ET DROP Dshield Block Listed Source	1
13.92.178.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.109.30.97	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	34
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.168.181.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.32.179.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
66.249.66.129	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.191	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
174.27.4.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.0.112.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.30.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.201.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
120.210.173.161	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.208.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.129.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.169.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.26.189	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.13.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
207.46.13.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
40.77.167.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.65.25.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.82.65.82	Netherlands	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.13.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.96	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.53.13.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
120.132.84.157	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.30.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.122	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.165	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-20-2016-07:04:04 to 04-20-2016-08:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.218.206.84	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.55.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.53.155.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.176	Block	8
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	8
79.183.118.82	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	3
95.35.192.184	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
2.55.24.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
64.62.219.156	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
79.183.118.82	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 79.183.118.82	Block	2
85.250.47.170	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.250.47.170	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15198-	Block	1
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
92.39.60.8	Moldova, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	1
141.212.122.161	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
91.109.30.97	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 91.109.30.97	Block	1
73.25.158.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
37.26.147.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
79.183.239.121	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/articles/mobile	Block	1
64.62.219.155	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.89	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
91.109.30.97	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/mobile	Block	1
76.117.226.86	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authentication-service.aspx/getauthservice	Block	1
37.26.149.147	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
104.128.144.131	Canada	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
80.178.203.34	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
64.62.219.155	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
188.165.233.34	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.165.233.34	Block	1
91.109.30.97	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 91.109.30.97	Block	1
40.77.167.85	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
123.59.59.52	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.qunar.com/894-he/nakhal.aspx	Block	1
80.246.130.71	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
188.165.233.34	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
91.109.30.97	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/11772.jpg	Block	1
141.212.122.161	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1