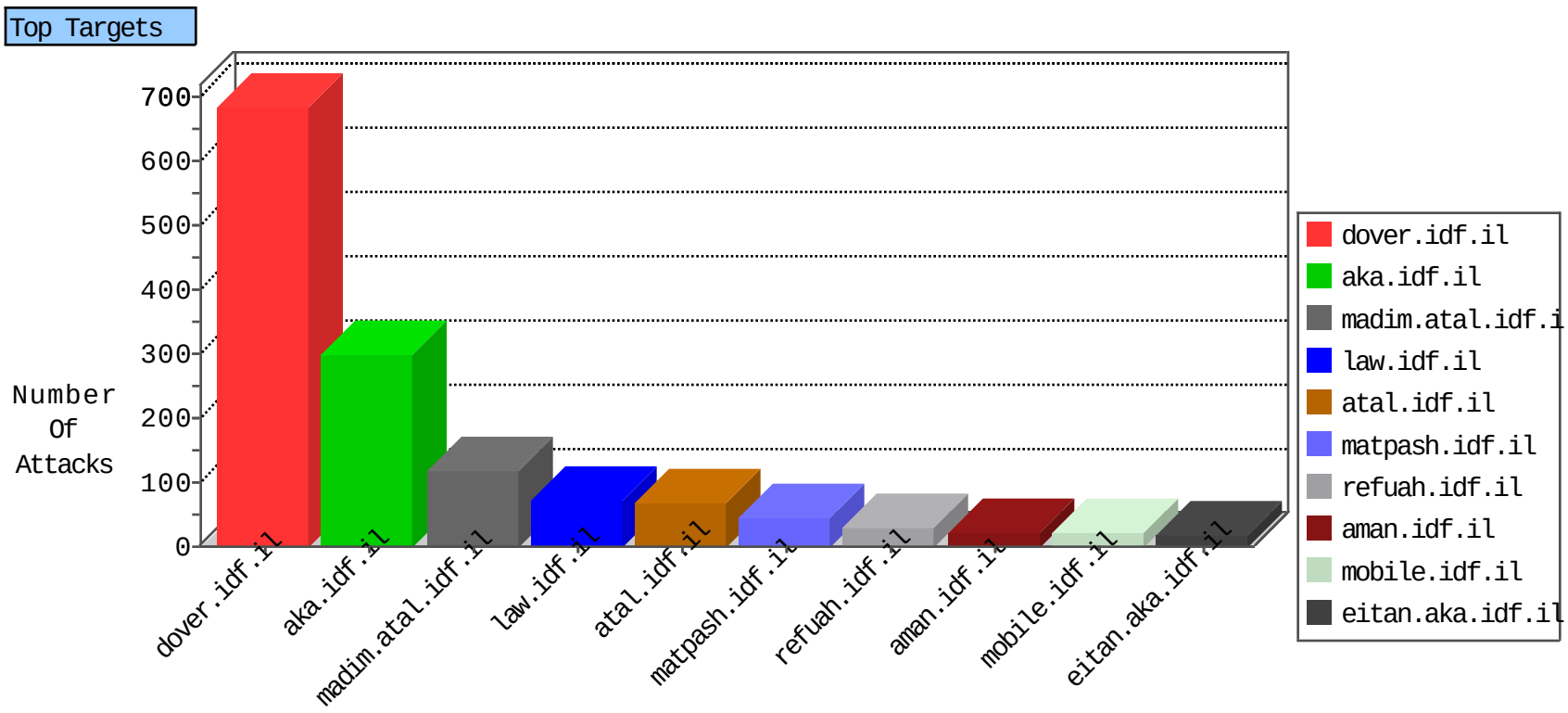
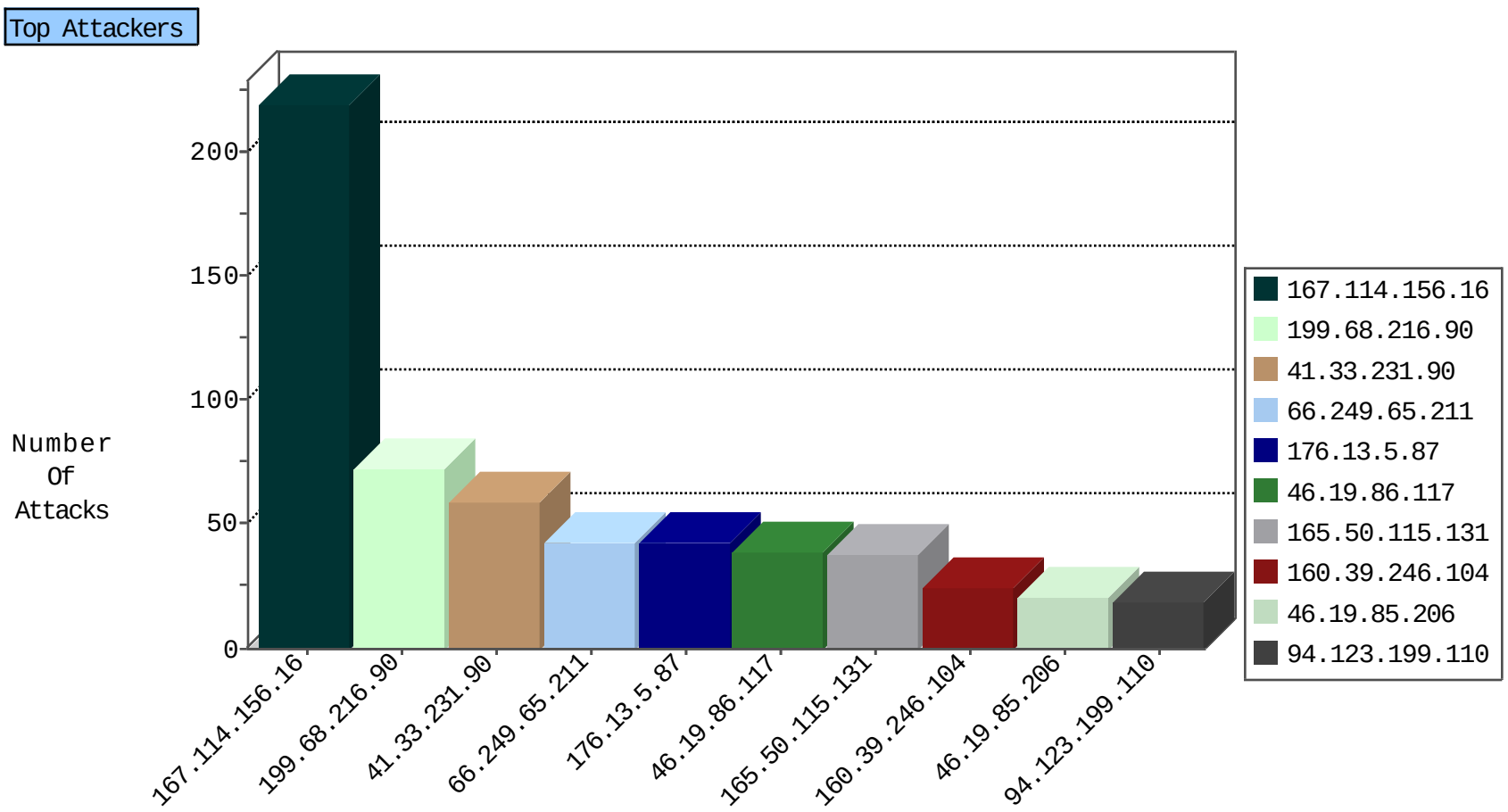
04-21-2016-18:04:04 to 04-21-2016-19:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-21-2016-18:04:04 to 04-21-2016-19:04:04

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	8544
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2413
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2395
37.26.146.240	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1573
212.14.228.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	663
109.186.30.39	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
66.249.65.211	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
141.228.106.147	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.125.129.75	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
199.68.216.90	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
202.88.1.3	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.212.122.204	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-21-2016-18:04:04 to 04-21-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-18:04:04 to 04-21-2016-19:04:04

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
61.180.240.202	147.237.76.38	China	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
80.82.78.38	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
218.86.103.146	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.249.172.97	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.123.199.110	147.237.77.176	Turkey	matpash.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	1
82.166.184.187	147.237.77.212	Israel	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
76.181.249.213	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.211.11	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
14.158.146.183	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.57.104.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.123.199.110	147.237.77.176	Turkey	matpash.idf.il	SERVER-WEBAPP admin.php access	1
85.250.74.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-21-2016-18:04:04 to 04-21-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.68.216.90	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	71
66.249.65.211	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
165.50.115.131	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
160.39.246.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
129.59.122.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.140.137.52	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.102.254.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
86.104.164.99	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
79.182.48.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.13.13.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.116.23.126	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
141.228.106.147	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
216.185.39.161	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
188.161.1.39	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.0.14.127	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.53.33.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.26.183.67	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.193	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.231	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
54.240.197.233	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.126.226	Israel	147.237.0.200	m4u.idf.il	drop		drop	6
95.86.116.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
141.228.106.148	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.228	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.89.217.234	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.225	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
79.183.160.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	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
2.55.54.177	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.126.226	Israel	147.237.0.35	akaws.idf.il	drop		drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	5
46.19.85.218	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.89.217.233	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4

04-21-2016-18:04:04 to 04-21-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
85.64.3.84	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.3.84	Block	11
46.118.156.3	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	8
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	6
207.232.36.85	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.232.36.85	Block	6
5.22.135.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
94.123.199.110	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 94.123.199.110	Block	6
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	6
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
94.123.199.110	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	5
94.123.199.110	Turkey	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 94.123.199.110	Block	4
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.55.151.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.11.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.173.231.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.42.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
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	2
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.211	Block	2
31.168.183.34	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/mobile	Block	2
200.79.13.211	Mexico	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	2
37.26.147.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.94.64.166	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	2
109.67.22.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.32.54	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
109.253.218.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.152.239.93	Portugal	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
85.64.3.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	1
134.249.55.100	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	1
89.152.239.93	Portugal	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
2.53.33.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.232.36.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
79.180.245.250	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
85.64.148.209	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/redirects/ssl-redirect.html	Block	1
195.93.234.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/rabanut/scriptresource.axd	None	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
149.50.12.164	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11139-	Block	1
2.53.37.169	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.183.30.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.28.175.172	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
94.123.199.110	Turkey	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
85.65.25.46	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 127.0.0.1/callback.json	Block	1
66.249.65.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
149.88.39.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
94.123.199.110	Turkey	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
179.33.75.0	Colombia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1

04-21-2016-18:04:04 to 04-21-2016-19:04:04