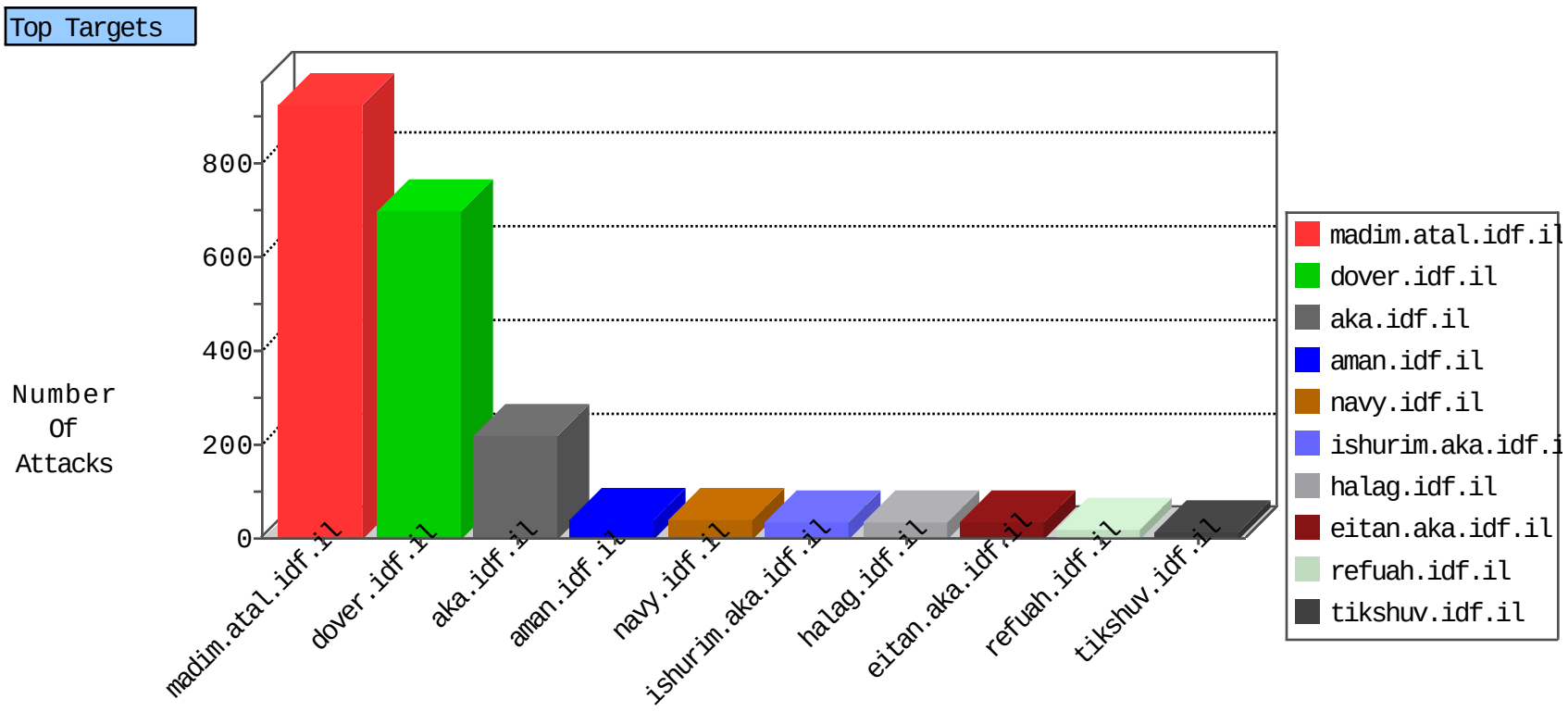
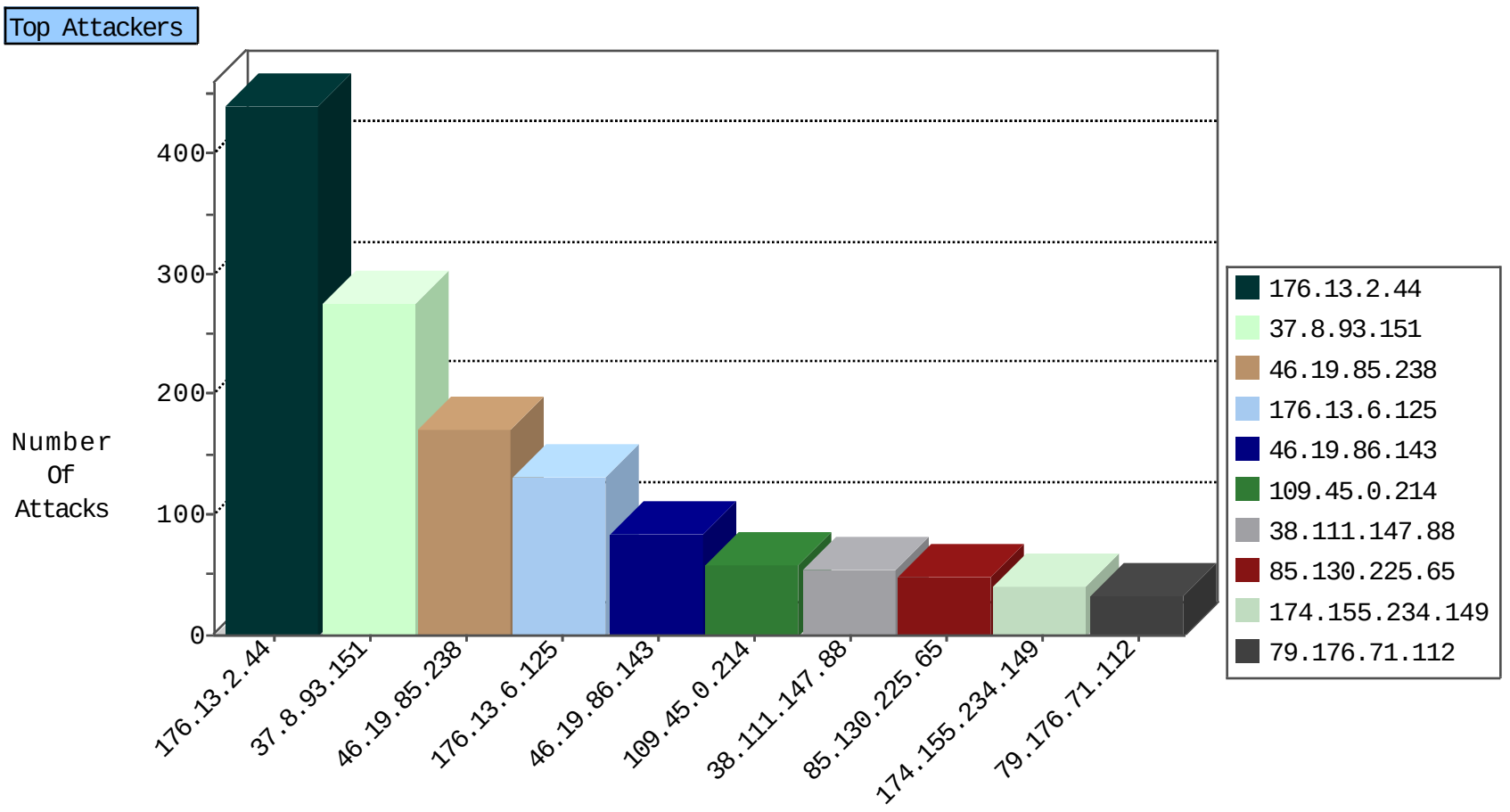
04-20-2016-17:04:01 to 04-20-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-20-2016-17:04:01 to 04-20-2016-18:04:01

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	6783
70.192.210.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3264
81.218.65.210	Israel	147.237.77.176	matpash.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	3
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
120.132.50.135	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-20-2016-17:04:01 to 04-20-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.132.168.32	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

04-20-2016-17:04:01 to 04-20-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.8.93.151	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP login.htm access	8
37.8.93.151	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP admin.php access	6
37.8.93.151	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP adminlogin access	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
120.37.66.198	147.237.77.216	China	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
87.69.115.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.10.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.211.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.241.229.102	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
190.79.95.237	147.237.72.166	Venezuela	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.161.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
62.128.48.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.125.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-20-2016-17:04:01 to 04-20-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.2.44	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	200
176.13.2.44	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	100
109.45.0.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
79.176.71.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.180.198.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
174.155.234.149	United States	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.0	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
73.136.136.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
174.155.234.149	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.65.42.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.225.65	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
109.253.194.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
85.130.225.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.130.225.65	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.53.181.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.140	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.225.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.145.211.54	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.219.128.187	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	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
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.181.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.89	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.168.204.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
111.69.53.98	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.225.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.147.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.225.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.144.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.47.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
176.13.2.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
176.13.6.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
37.8.93.151	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.93.151	Block	97
37.8.93.151	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	91
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
37.8.93.151	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	70
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.149.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.53.163.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.53.140.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
178.214.69.158	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	3
46.210.168.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
120.37.66.198	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.37.66.198	Block	3
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.15.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.1.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.155.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
120.37.66.198	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 1.7.1445480999.1445480999.; in URL asp.net_sessionid=v2h1hz21fzred4u050tqdtj2	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.253.220.221	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/catalog/catalog.aspx	Block	1
79.177.128.142	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=1%7C16; __atuvs=5717989ce6a907fd000	Block	1
84.200.45.173	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.115.130.253	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
155.201.35.63	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.149.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
117.25.108.125	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/trackback/	Block	1
79.178.168.79	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/faq/mobile	Block	1
2.55.29.41	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
144.76.8.132	Germany	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 144.76.8.132	Block	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Malformed URL asp.net_sessionid=v2h1hz21fzred4u050tqdtj2;	Block	1
37.8.93.151	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1
90.171.36.99	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.53.59.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
213.8.63.16	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
120.37.66.198	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1