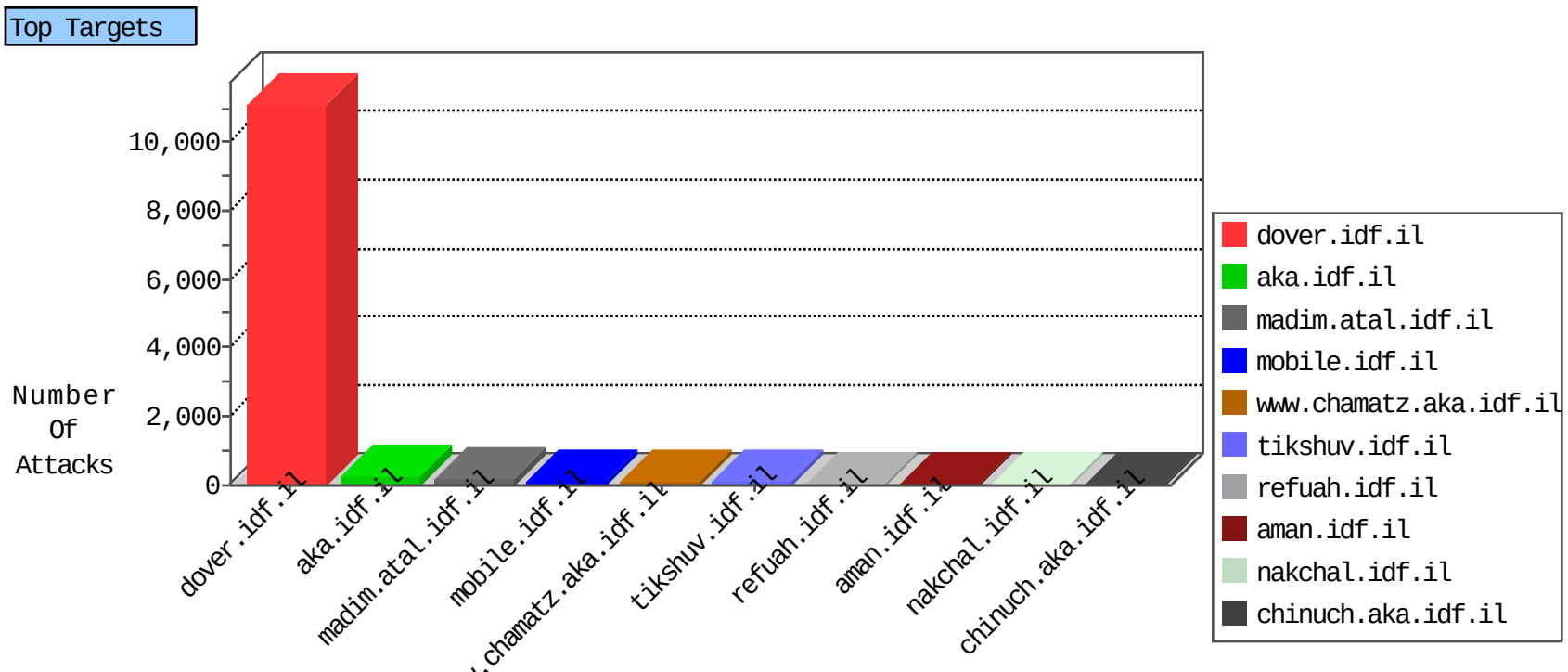
04-07-2016-12:04:09 to 04-07-2016-13:04:09

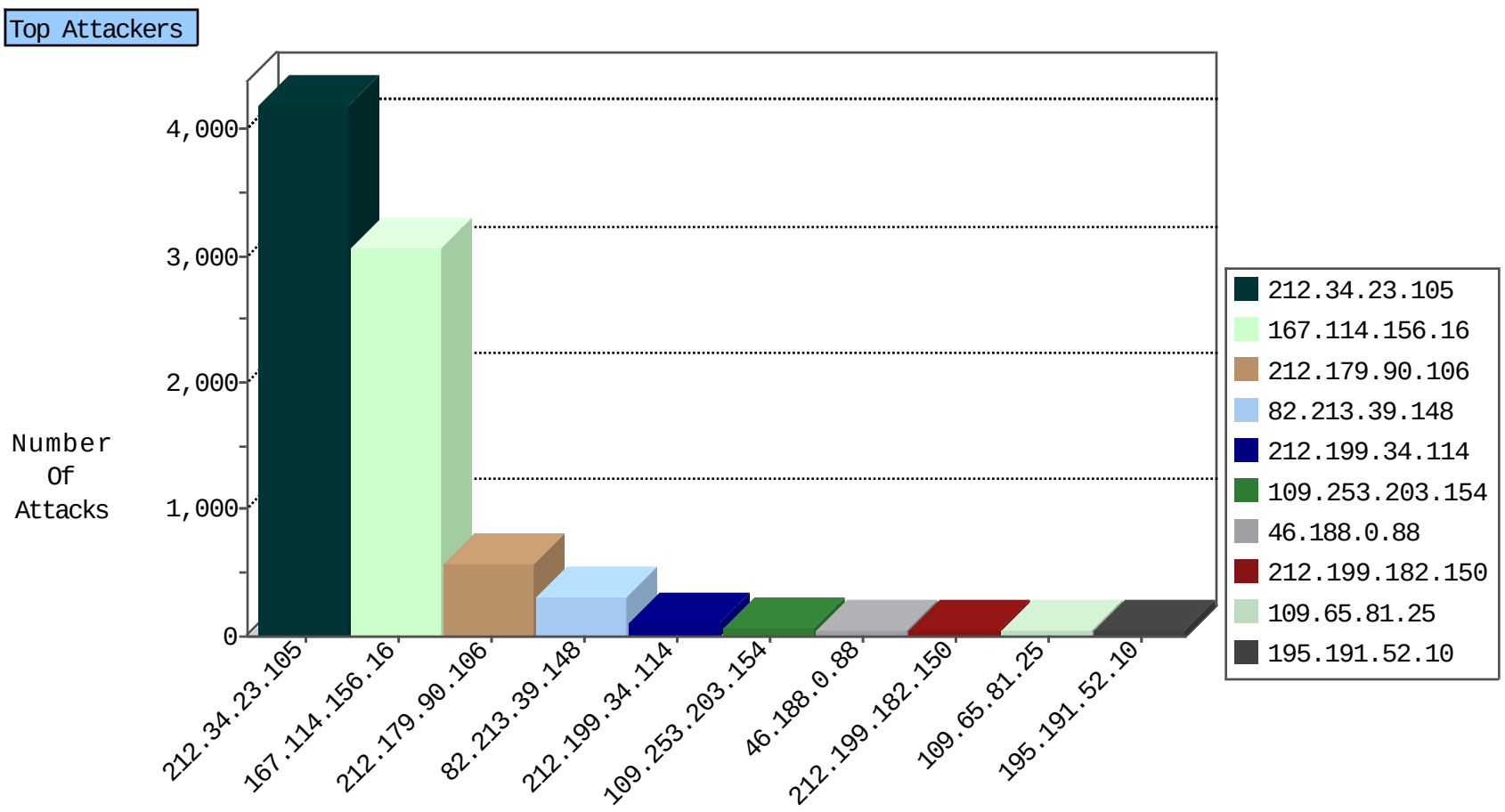
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-07-2016-12:04:09 to 04-07-2016-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	448870
212.34.23.105	Jordan	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	24879
182.140.230.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20091
212.34.23.105	Jordan	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	18467
212.34.23.105	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11823
87.70.21.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6439
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3053
212.34.23.105	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	484
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
31.168.170.222	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.170.222	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.70.184.164	Netherlands	147.237.77.205	prisha.idf.il	L4 Source or Dest Port Zero	drop	1
82.145.216.254	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
82.145.218.157	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
185.70.184.164	Netherlands	147.237.76.198	e.yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
185.70.184.164	Netherlands	147.237.77.179	e.mazi.idf.il	L4 Source or Dest Port Zero	drop	1

04-07-2016-12:04:09 to 04-07-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.81.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.181.108.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
2.55.33.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.67.22.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.253.130.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.79.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.120.126.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.90.118	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.61.21	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.68.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-12:04:09 to 04-07-2016-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.174.93.96	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
87.70.21.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.34.23.105	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.221.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.88.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.138.113.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.245.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.58.132.26	147.237.76.31	Spain	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
77.124.16.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.23.175.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.245.129.39	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
122.141.236.69	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1

04-07-2016-12:04:09 to 04-07-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	578
82.213.39.148	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	301
212.199.34.114	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	91
46.188.0.88	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
195.191.52.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.65.81.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.81.44.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
141.0.15.176	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
91.183.186.227	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
84.94.193.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
109.253.130.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
84.95.2.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.121.111.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.55.39.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
80.246.130.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
85.140.2.118	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.253	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.253.129.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
87.70.21.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.176.34.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.28.191.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.182.176.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
31.168.11.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.67.43.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
207.46.13.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.203.154	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter RepeatPassword	Block	62
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
80.246.137.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
2.52.145.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.55.14.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.220.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
87.71.45.121	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.55.45.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.136.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.129.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
2.54.189.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.205.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.249.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.7.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	2
171.8.167.61	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
109.253.129.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.172.191.135	Poland	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/forum	Block	2
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.157.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.157.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.114.91.234	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
46.30.167.177	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
171.8.167.73	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
37.227.43.60	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.235.98.139	Block	1
85.65.217.122	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.34.20.117	Jordan	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
182.140.230.15	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
164.132.182.30	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
27.221.19.15	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
109.65.99.68	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.139.169	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.114.91.234	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
46.19.85.39	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.34.20.117	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method ww.cogat.idf.il in URL	Block	1
188.64.222.101	Russian Federation	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
27.221.19.22	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
2.52.130.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1