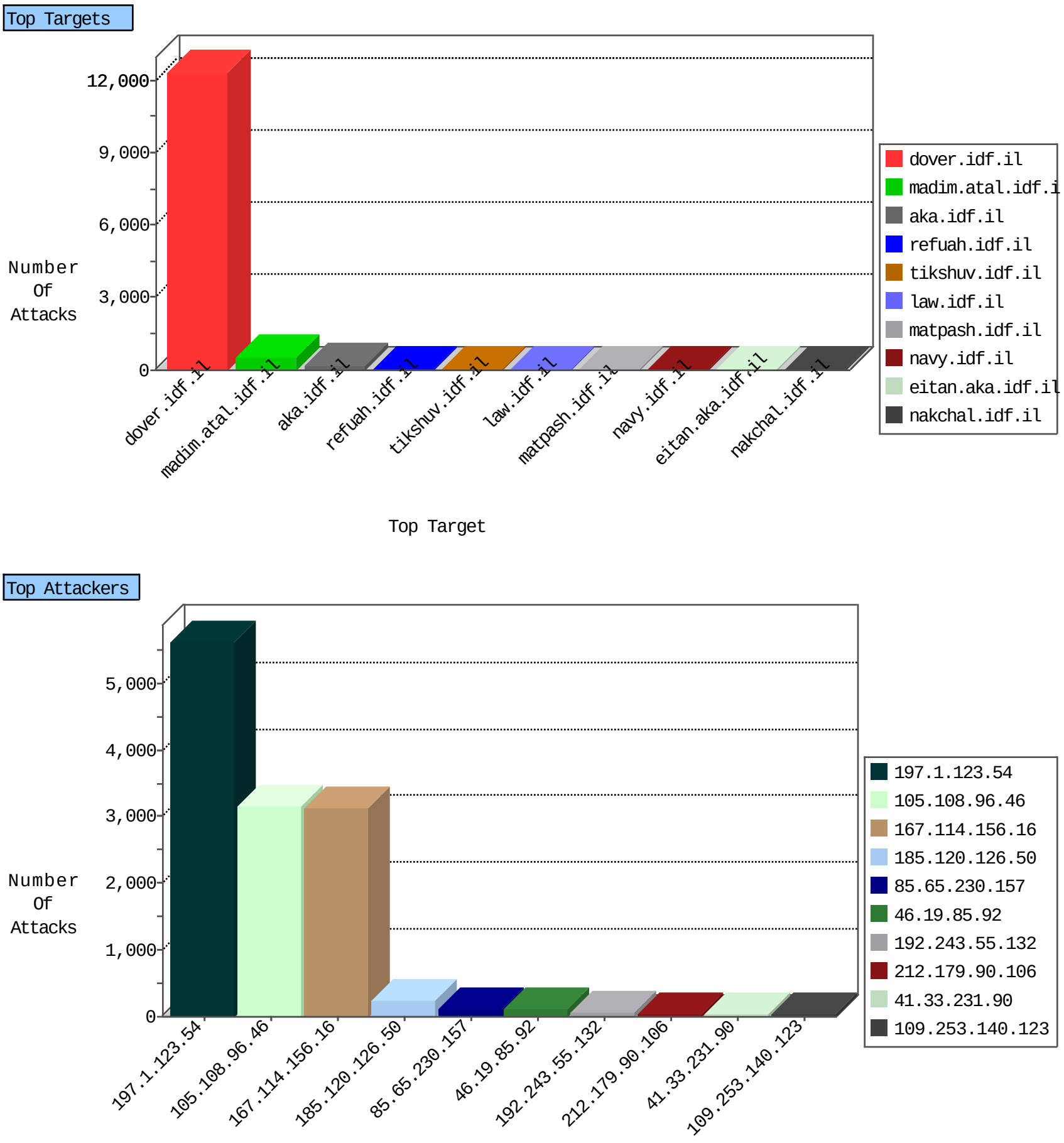
04-11-2016-20:04:09 to 04-11-2016-21:04:09

IDF Under Attack Daily Report



04-11-2016-20:04:09 to 04-11-2016-21:04:09

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_Ip_Web_In	drop	3139
46.244.157.134	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	514
79.180.9.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	280
85.65.48.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	114
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	55
79.179.54.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
24.114.40.155	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
149.50.117.181	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
176.13.16.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
24.184.154.206	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
213.57.213.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.219.130	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
46.19.85.64	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
77.126.174.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.162	China	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
37.26.146.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
162.216.114.158	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
2.53.50.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
37.128.85.37	Poland	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
79.233.230.70	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-11-2016-20:04:09 to 04-11-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.121.67.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
31.154.31.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.138.38.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
36.110.147.78	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.13.3.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-11-2016-20:04:09 to 04-11-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
106.187.37.163	147.237.77.216	Japan	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
107.158.255.194	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1

04-11-2016-20:04:09 to 04-11-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3017
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2911
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2591
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	drop		drop	171
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
185.120.125.43	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop		drop	13
149.78.242.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.28.152.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.131.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.121.198.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.92.182.124		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.204	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
84.228.224.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence		monitor	6
68.194.87.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.52.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack		reject	6
5.28.131.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
31.210.186.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.90.66.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.244.157.134	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
204.236.237.61	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.225	Israel	147.237.76.86	navy.idf.il	SYN Attack		reject	4
45.244.84.151	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.85.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.137.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.51.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.138.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
79.233.230.70	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

04-11-2016-20:04:09 to 04-11-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	236
85.65.230.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
109.253.140.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.253.129.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
65.55.210.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
87.70.63.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
199.30.25.78	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.12.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.141.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
157.55.2.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.8.68.239	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
199.30.24.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
157.55.12.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
17.142.155.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	2
149.78.242.159	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.22.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.151.198.129	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ 994-8992-en / navy.aspx	Block	2
68.194.87.109	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
46.120.13.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.228.224.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.126.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.228.224.161	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
54.153.33.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
95.86.106.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.180.174.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
207.46.13.62	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
65.55.210.244	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
114.97.195.129	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1570-ar/idfg.aspx/trackback/	Block	1
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
85.65.94.195	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
62.210.162.37	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
154.16.138.15	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
97.121.151.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.182.128.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/עטוד	Block	1
207.46.13.144	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
178.255.87.242	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/robots.txt	Block	1
66.249.64.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/master/script	Block	1
131.253.25.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.168.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1

04-11-2016-20:04:09 to 04-11-2016-21:04:09