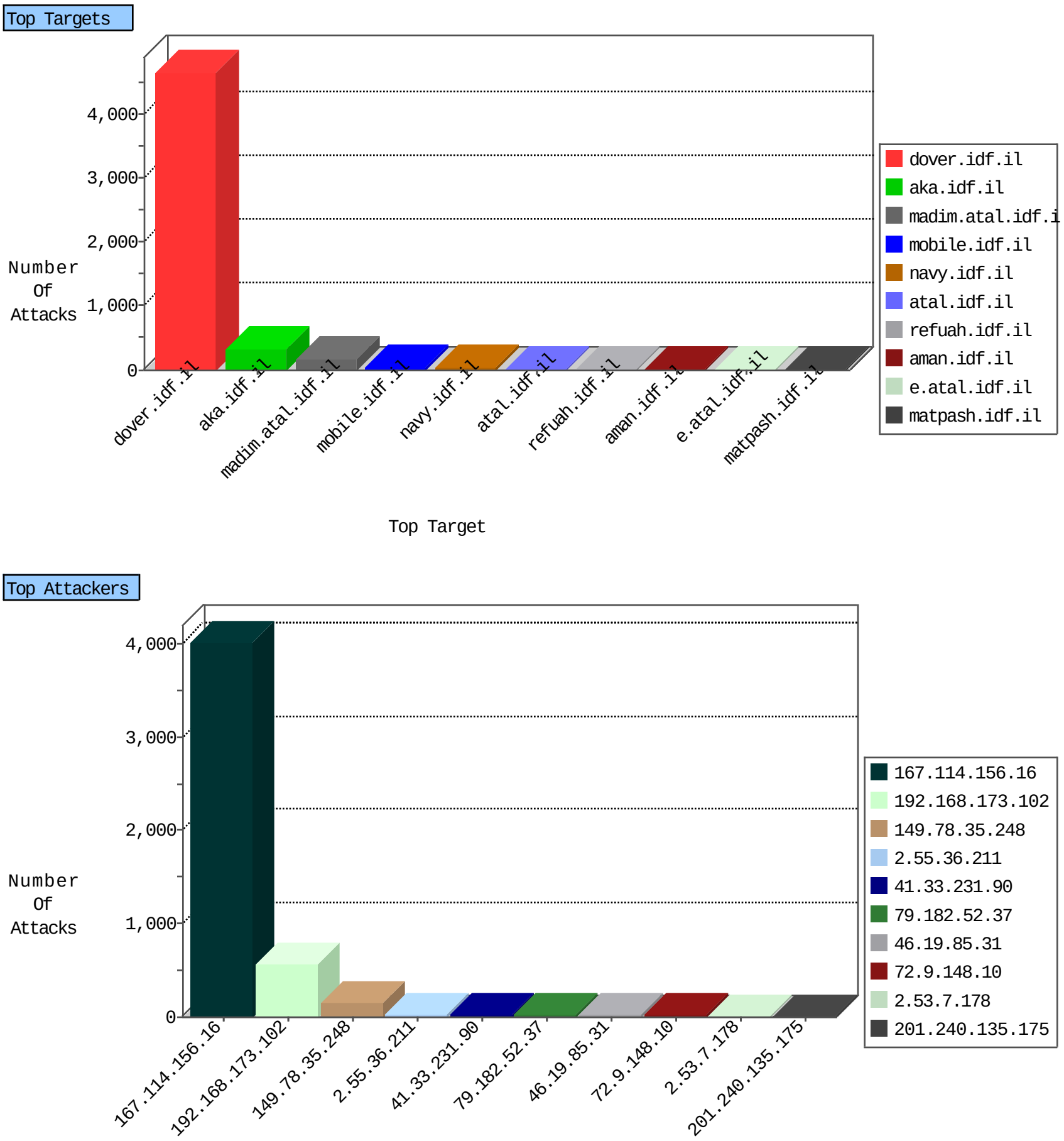
04-08-2016-17:04:06 to 04-08-2016-18:04:06

IDF Under Attack Daily Report



04-08-2016-17:04:06 to 04-08-2016-18:04:06

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	4028
109.67.147.213	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
201.240.135.175	Peru	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-08-2016-17:04:06 to 04-08-2016-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.50.130.135	Singapore	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-17:04:06 to 04-08-2016-18:04:06

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
79.177.179.182	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
216.227.58.7	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
208.100.26.228	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.56.166.188	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.95.73	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
216.227.58.7	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
188.161.118.232	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.205.127.156	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP login.htm access	1
64.13.147.226	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-08-2016-17:04:06 to 04-08-2016-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	377
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	182
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.53.7.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
79.182.52.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.102.254.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.189.190.212	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
201.240.135.175	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
149.78.32.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.94.96.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
173.49.136.5	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.55.36.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.36.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
64.233.173.128	Asia/Pacific Region	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
2.55.36.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.55.36.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.182.52.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
207.46.13.36	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.176.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.190.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.117.243.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.22.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
201.240.135.175	Peru	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.124.4.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.117.76.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.147.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.52.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.53.35.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.182.1.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
216.145.11.94	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
46.19.86.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.14.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.33.169.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.62.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.86.117.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.137.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.148.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.67.5.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.187.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-08-2016-17:04:06 to 04-08-2016-18:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.35.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
199.30.25.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
2.55.36.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.180.68.193	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
176.13.21.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.169.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.105.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	3
79.180.68.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.136.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.139.86	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8990	Block	2
176.13.4.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
129.45.43.114	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.54.184.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.66.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.13.113.93	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
92.84.131.189	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
207.46.13.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.82.47.3	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
41.40.210.19	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.4.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
130.209.6.42	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
79.182.52.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
157.55.39.111	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
37.8.14.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.252.91.253	Russian Federation	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
76.31.170.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
213.87.103.139	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
46.117.243.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
130.209.6.42	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-en/	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
199.30.25.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.25	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/home/default.asp	None	1
109.252.91.253	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
213.87.103.139	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
54.153.32.246	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
141.0.12.104	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22787-ar/dover.aspx'	Block	1
23.81.235.219	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
82.205.127.156	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login	Block	1
201.240.135.175	Peru	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 201.240.135.175 (Open Mode)	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
41.40.134.48	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.26	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
31.13.110.123	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

04-08-2016-17:04:06 to 04-08-2016-18:04:06