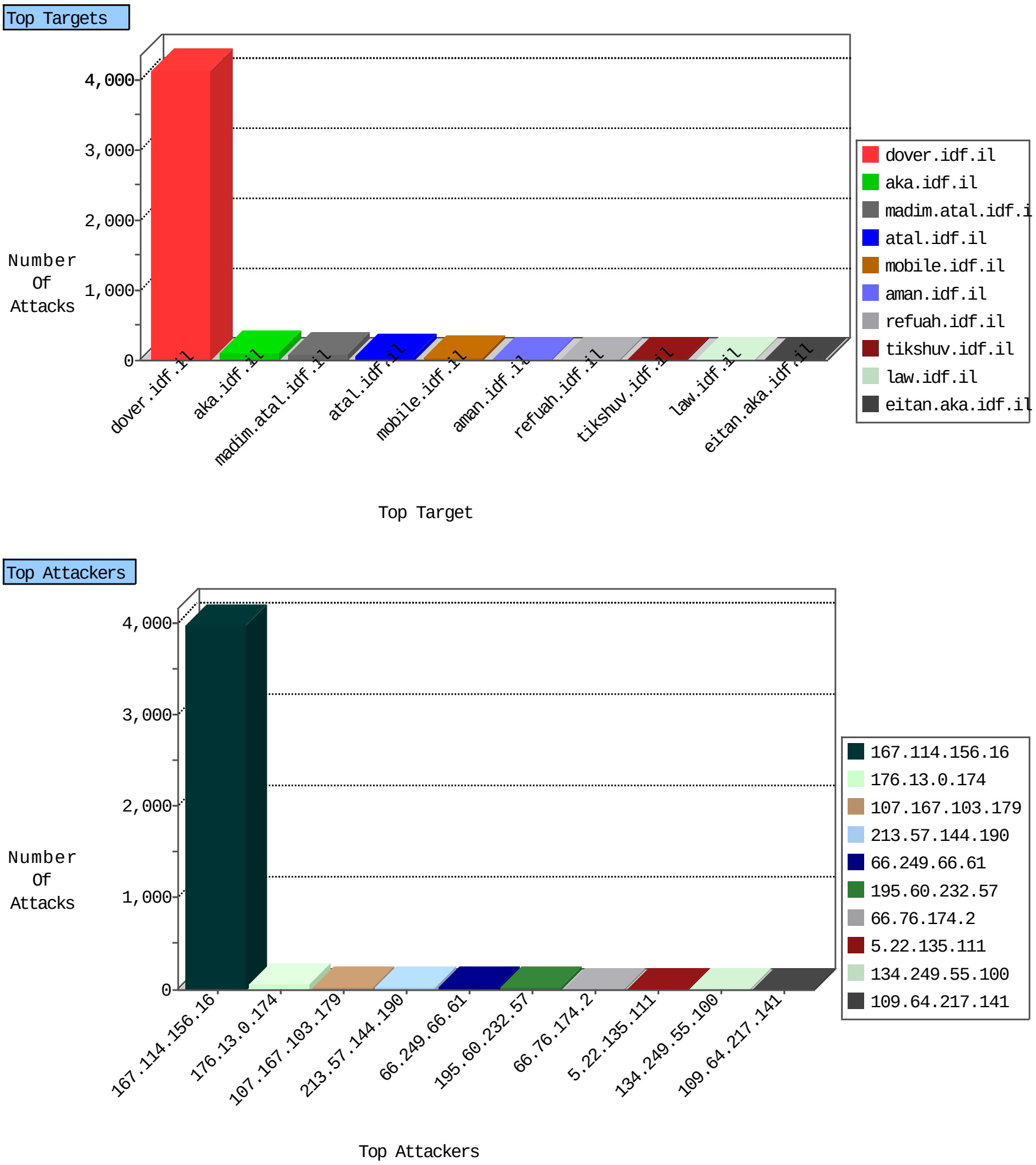
04-18-2016-23:04:08 to 04-19-2016-00:04:08

IDF Under Attack Daily Report



04-18-2016-23:04:08 to 04-19-2016-00:04:08

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	3972
82.145.217.182	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
198.48.92.104	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.162	China	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-18-2016-23:04:08 to 04-19-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.76.174.2	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-18-2016-23:04:08 to 04-19-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.76.174.2	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
109.67.144.183	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
93.179.68.181	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
121.40.195.144	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
61.82.224.213	147.237.8.27	Korea, Republic of	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.3.202.115	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.76.86	Japan	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-18-2016-23:04:08 to 04-19-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
107.167.103.179	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
213.57.144.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.64.217.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.149.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.156.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.246.49.97	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	8
149.50.41.173	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.17.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
2.53.51.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.173.255	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
149.88.125.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
190.210.74.49	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.45.65.196	Netherlands	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
68.179.80.21	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.210.225.135	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
108.67.169.124	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
184.173.233.226	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
77.124.22.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.89.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.125.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.125.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.9.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.235.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.14	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
152.115.70.227	Denmark	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	3
5.102.242.250	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.20	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.60.232.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.161.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.189.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.138.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.8.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.104.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.212.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.178.155.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.19	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
31.210.187.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-18-2016-23:04:08 to 04-19-2016-00:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.22.134.202	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.172	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

04-18-2016-23:04:08 to 04-19-2016-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
134.249.55.100	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	11
5.22.135.111	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	9
46.118.156.3	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	8
52.63.114.146	Australia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.63.114.146	Block	4
2.53.13.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.12.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.157.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.146.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.62.231	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.113.99.244	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
109.253.139.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.46	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
94.23.54.167	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/blog/wp-admin/	Block	1
2.53.51.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
52.63.114.146	Australia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 52.63.114.146	Block	1
31.13.112.118	Ireland	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/1783-he/refuah.aspx'מצאת	Block	1
109.253.156.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.138.243	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 81.218.138.243	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
198.71.230.46	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/wordpress/wp-admin/	Block	1
157.55.39.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
104.7.6.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
31.179.42.77	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
85.65.245.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.245.65	Block	1
208.113.155.2	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.69.69	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1926-he/cogat.aspx	Block	1
157.55.39.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.0	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
2.55.149.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.186.113.132	Japan	147.237.76.86	navy.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
54.79.76.74	Australia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
85.65.245.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
213.57.144.190	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
157.55.39.248	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sachar/forgotpassword.aspx	Block	1
40.77.167.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.149.184	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
109.226.43.146	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.208.180.12	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/old/wp-admin/	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;w in www.aka.idf.il/main/giyus/captcha.ashx	None	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
37.26.149.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

04-18-2016-23:04:08 to 04-19-2016-00:04:08