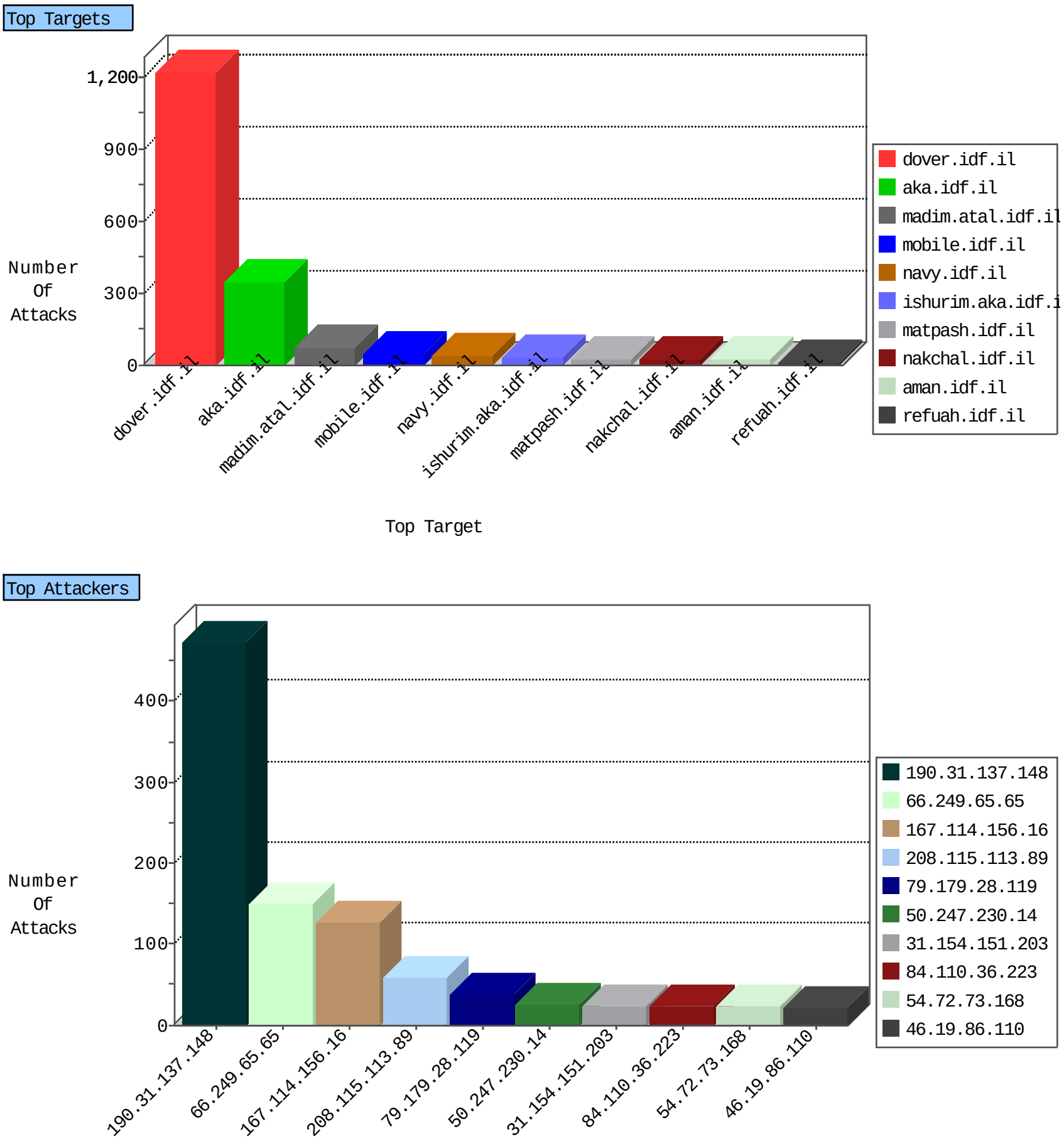
05-03-2016-19:04:01 to 05-03-2016-20:04:01

IDF Under Attack Daily Report



05-03-2016-19:04:01 to 05-03-2016-20:04:01

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	HTTP-POST-Segmented-DoS	dest-reset	5570
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1908
197.160.71.6	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	16
190.31.137.148	Argentina	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-19:04:01 to 05-03-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.160.71.6	Egypt	147.237.77.216	dover.idf.i	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2

05-03-2016-19:04:01 to 05-03-2016-20:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.71.40.159	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	14
5.101.156.42	147.237.72.166	Russian Federation	aka.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
45.62.254.172	147.237.77.243	Canada	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.40.4.41	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.62.254.172	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.105.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.62.254.172	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.52.47	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.254.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.216.3.101	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.29.84.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.141.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.103.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.195.83.66	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
45.62.254.172	147.237.77.235	Canada	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
45.62.254.172	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
37.26.147.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.240.80.14	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.116.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.150.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.114.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.221.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-19:04:01 to 05-03-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
190.31.137.148	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	464
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
79.179.28.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
84.110.36.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.247.230.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.26.149.135	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.133.93.187	Ukraine	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
91.240.80.14	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.126.235.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.162.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.115.52.201	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.145.216.115	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.130	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.193.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.222.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
62.0.222.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.209.131	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.240	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.75	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.50.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
35.248.29.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.129.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.227.25.109	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

05-03-2016-19:04:01 to 05-03-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.151.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
185.3.147.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
131.253.25.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
109.67.109.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	6
109.67.109.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.129.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.138.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.35.160	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.35.160	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.7.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.60	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
5.101.156.42	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx?catid=62471&amp	Block	2
50.247.230.14	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.240.80.14	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.36.49	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
217.132.38.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.101.156.42	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter categoryID in www.aka.idf.il/main/home/default.aspx	None	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
198.163.212.12	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
141.212.122.145	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
37.26.147.152	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.79.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
188.237.250.4	Moldova, Republic of	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
109.253.159.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/תאריך יום השו אה /2016giyus	Block	1
5.101.156.42	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter categoryID in www.aka.idf.il/main/rabanut/	None	1
79.176.26.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.116.182.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.131	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
2.53.142.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1538	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10050-en	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
46.117.35.160	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
188.237.250.4	Moldova, Republic of	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
87.70.45.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/	None	1
185.3.147.145	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.3.147.145	Block	1
109.67.109.207	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.67.109.207	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8876-he/refuah.aspx	Block	1
188.237.250.4	Moldova, Republic of	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
31.154.151.151	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
213.254.241.6	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1727	Block	1
46.19.85.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

05-03-2016-19:04:01 to 05-03-2016-20:04:01