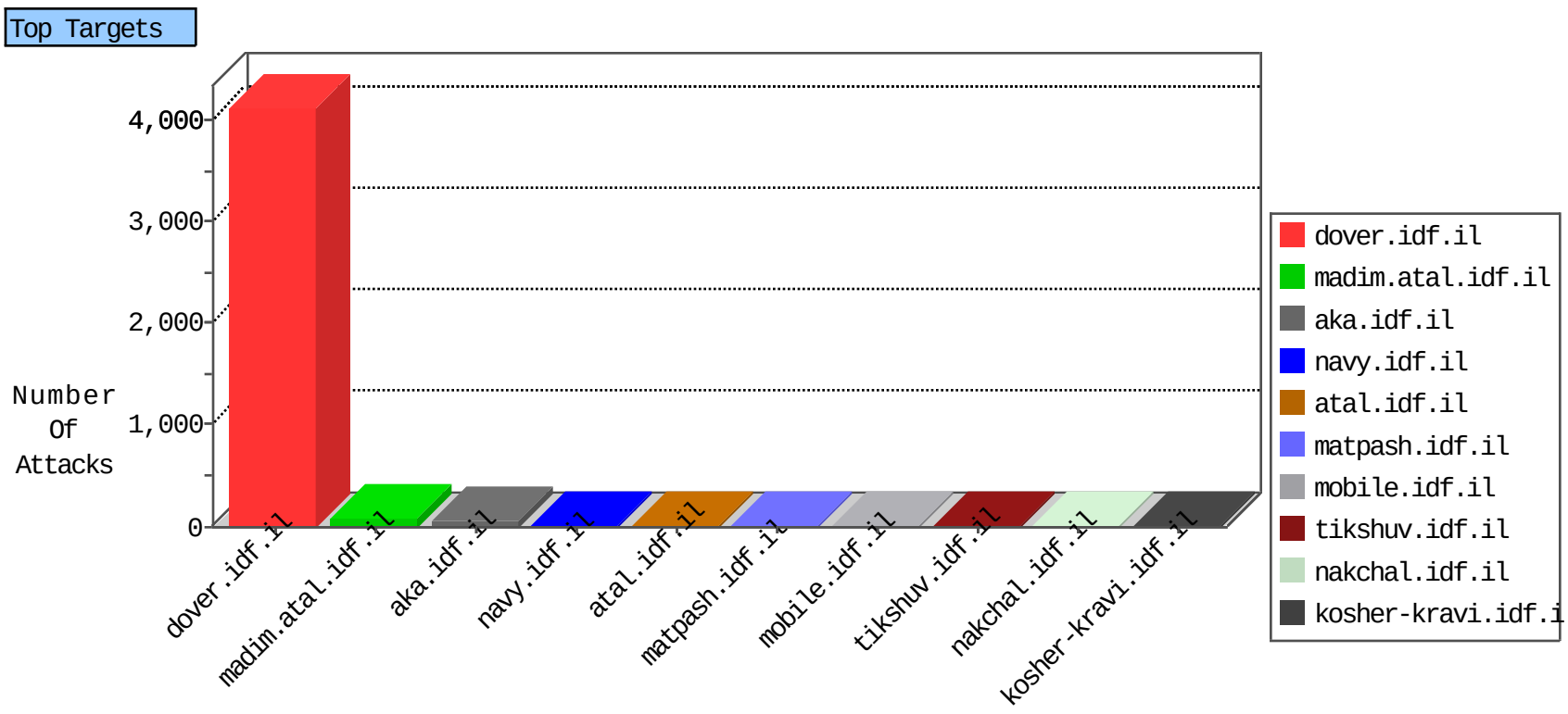
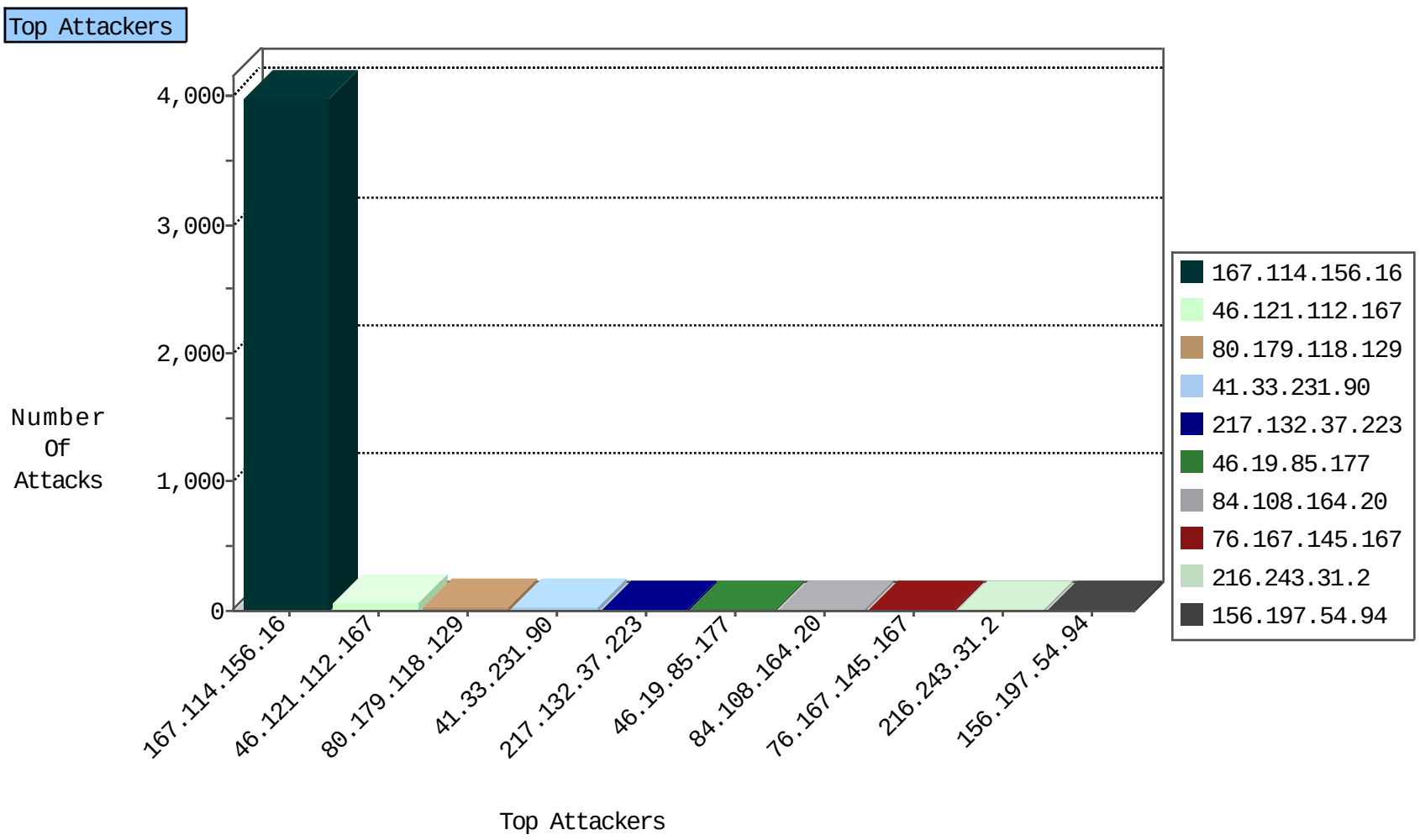
04-15-2016-22:04:05 to 04-15-2016-23:04:05

IDF Under Attack Daily Report





04-15-2016-22:04:05 to 04-15-2016-23:04:05

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	3978
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
134.147.203.115	Germany	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	2
37.230.210.153	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
94.102.52.10	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.147	chinuch.aka.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
94.102.52.10	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
14.186.40.68	Vietnam	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.17.11	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
46.55.56.133	Moldova, Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-15-2016-22:04:05 to 04-15-2016-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.142	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
106.120.173.139	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
84.229.28.153	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
84.228.19.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-22:04:05 to 04-15-2016-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
156.197.54.94	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	8
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
151.11.201.3	147.237.77.234	Italy	halag.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.243	Kazakstan	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.77.243	Kazakstan	mobile.idf.il	ET SCAN NMAP -f -sS	1
69.12.77.214	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.100.128	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
187.161.165.132	147.237.72.14	Mexico	dover.idf.il(old	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.11.201.3	147.237.77.234	Italy	halag.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.77.234	Italy	halag.idf.il	ET SCAN NMAP -f -sS	1
88.204.187.90	147.237.77.243	Kazakstan	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.8.24	Netherlands	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
13.92.100.128	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
218.57.11.7	147.237.76.38	China	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1

04-15-2016-22:04:05 to 04-15-2016-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
217.132.37.223	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
76.167.145.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
84.108.164.20	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.166.190.177	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.237.234.84	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.121.112.167	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
132.76.50.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.75.70	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
80.179.118.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.65.75.70	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.118.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.67.135.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.192.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.54.68	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.71.52.35	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.54.68	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.234.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.152.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.126.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
182.118.20.175	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.148.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.102.195.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
118.173.131.165	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
84.109.155.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.2.141	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.138.75.160	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.181.242.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
85.65.2.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
89.138.75.160	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.186.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.126.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.88.231.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.48	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.92.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
23.27.127.203	United States	147.237.0.33	idf.il	drop		drop	1
149.50.67.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.53.15.37	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
101.201.147.32	China	147.237.0.35	akaws.idf.il	drop		drop	1
84.109.155.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
156.197.54.94	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.112.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.228.26.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.134.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
37.120.18.89	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	2
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.62.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3416.jpg	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
37.120.18.89	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
108.61.117.164	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.89.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
120.39.4.174	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.39.4.174	Block	1
80.246.137.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$comboQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2662.jpg	Block	1
141.212.122.209	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.120.18.89	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
109.186.42.77	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
120.39.4.174	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
2.53.158.242	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.108.164.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.191	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.226.17.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/news.asp	Block	1
84.110.144.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.6.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
72.227.226.1	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-	Block	1
37.120.18.89	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.120.18.89	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
79.181.242.51	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

04-15-2016-22:04:05 to 04-15-2016-23:04:05