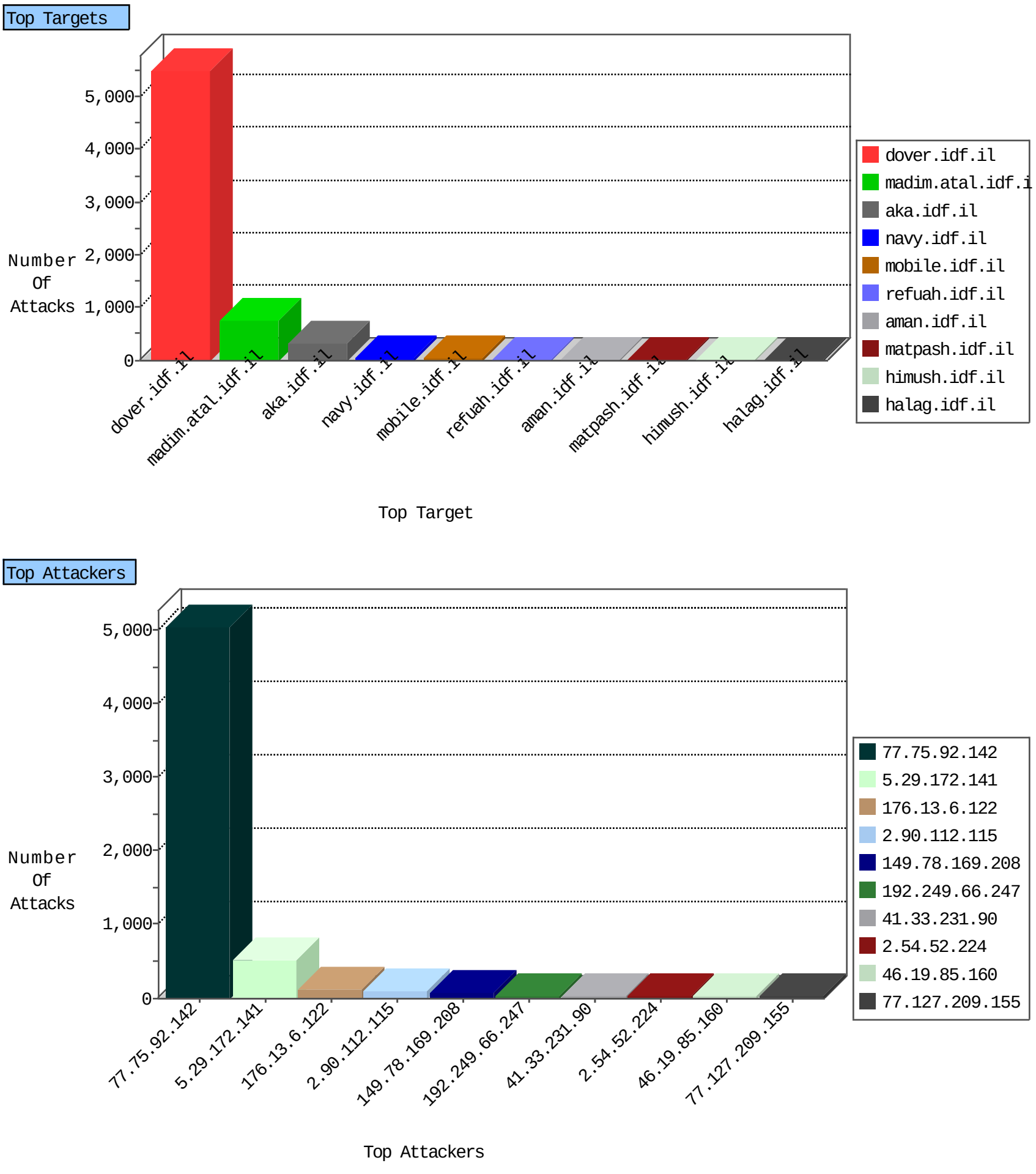
02-16-2016-19:04:09 to 02-16-2016-20:04:09

IDF Under Attack Daily Report



02-16-2016-19:04:09 to 02-16-2016-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	84613
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1329
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	294
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	125
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	82
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	17
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
93.85.70.99	Belarus	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
188.161.123.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
77.75.92.252	Lebanon	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.58.102.95	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
129.22.151.69	United States	147.237.76.201	e.atal.idf.i	Block_Udp_All_Nets	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
78.189.185.10	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-16-2016-19:04:09 to 02-16-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4

02-16-2016-19:04:09 to 02-16-2016-20:04:09

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
2.90.112.115	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From	4
2.90.112.115	147.237.77.216	Saudi Arabia	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
109.64.171.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
2.54.158.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.170.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.242.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.124.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
111.207.243.73	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
79.127.112.45	147.237.76.198	Iran, Islamic Republic of	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
61.182.170.38	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.79.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.25.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.90.112.115	147.237.77.216	Saudi Arabia	dover.idf.il	ET SCAN Vega Web Application Scan	1
213.57.72.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.244.113.114	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
188.161.123.44	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.213.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.251.21.227	147.237.72.166	Germany	aka.idf.il	portscan: TCP Distributed Portscan	1
79.127.112.45	147.237.76.198	Iran, Islamic Republic of	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.141.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.9.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
87.69.162.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.76.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.132.233	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.44.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-16-2016-19:04:09 to 02-16-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4589
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	59
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.178.170.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.39.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.133.247.134	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.54.52.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
31.210.186.250	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
188.161.123.44	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.201.7.248	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.182.11.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
188.120.148.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.65.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.52.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.126.105.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.105.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.1.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.65.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.13.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.160.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
77.125.120.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.52.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.142.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.123.44	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.54.37.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.228.21.219	Czech Republic	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
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.52.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.127.170.70	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.110	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.241.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.88.151.144	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.178.13.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-16-2016-19:04:09 to 02-16-2016-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	311
176.13.6.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	97
149.78.169.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.90.112.115	Block	14
93.172.24.9	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 93.172.24.9	Block	12
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
109.66.58.103	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.66.58.103	Block	10
213.57.225.123	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.57.225.123	Block	8
46.19.86.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	8
213.8.204.38	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	7
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1133-he/dover.aspx parameter PageNum	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	6
79.180.98.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.98.101	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	6
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	5
213.57.225.123	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	5
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.7.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.7.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.228.7.56	Block	3
109.253.156.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.98.101	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.24.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.6.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.218.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.228.7.56	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.66.108.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$118 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	2
199.30.25.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.39.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	2
91.226.4.171	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'	Block	2
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.0.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** *, Observed ********** ********** **********	None	1
84.228.135.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1842-he/dover.aspx	Block	1
79.183.22.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.90.112.115	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1379-he/dover.aspx	Block	1
93.172.24.9	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	1

02-16-2016-19:04:09 to 02-16-2016-20:04:09