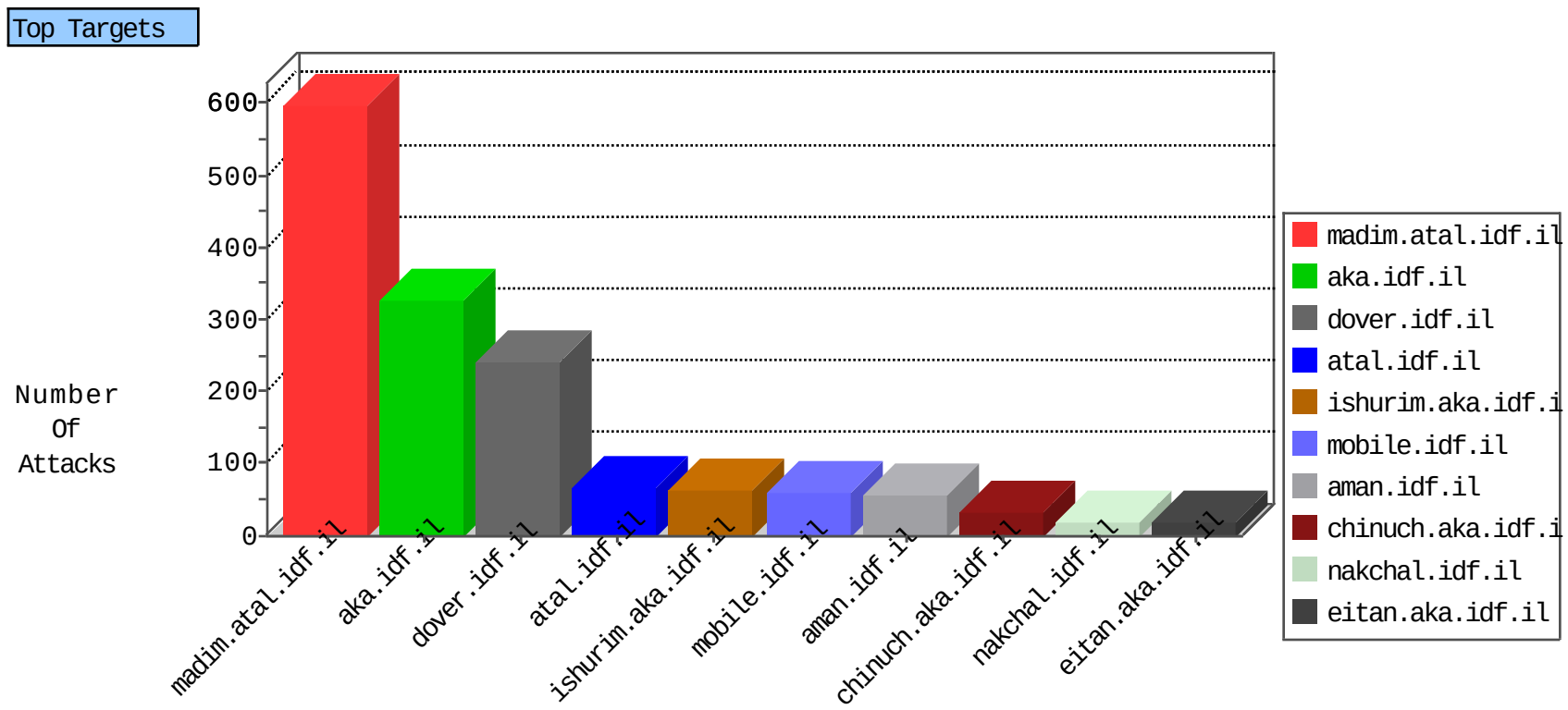
02-07-2016-12:04:07 to 02-07-2016-13:04:07

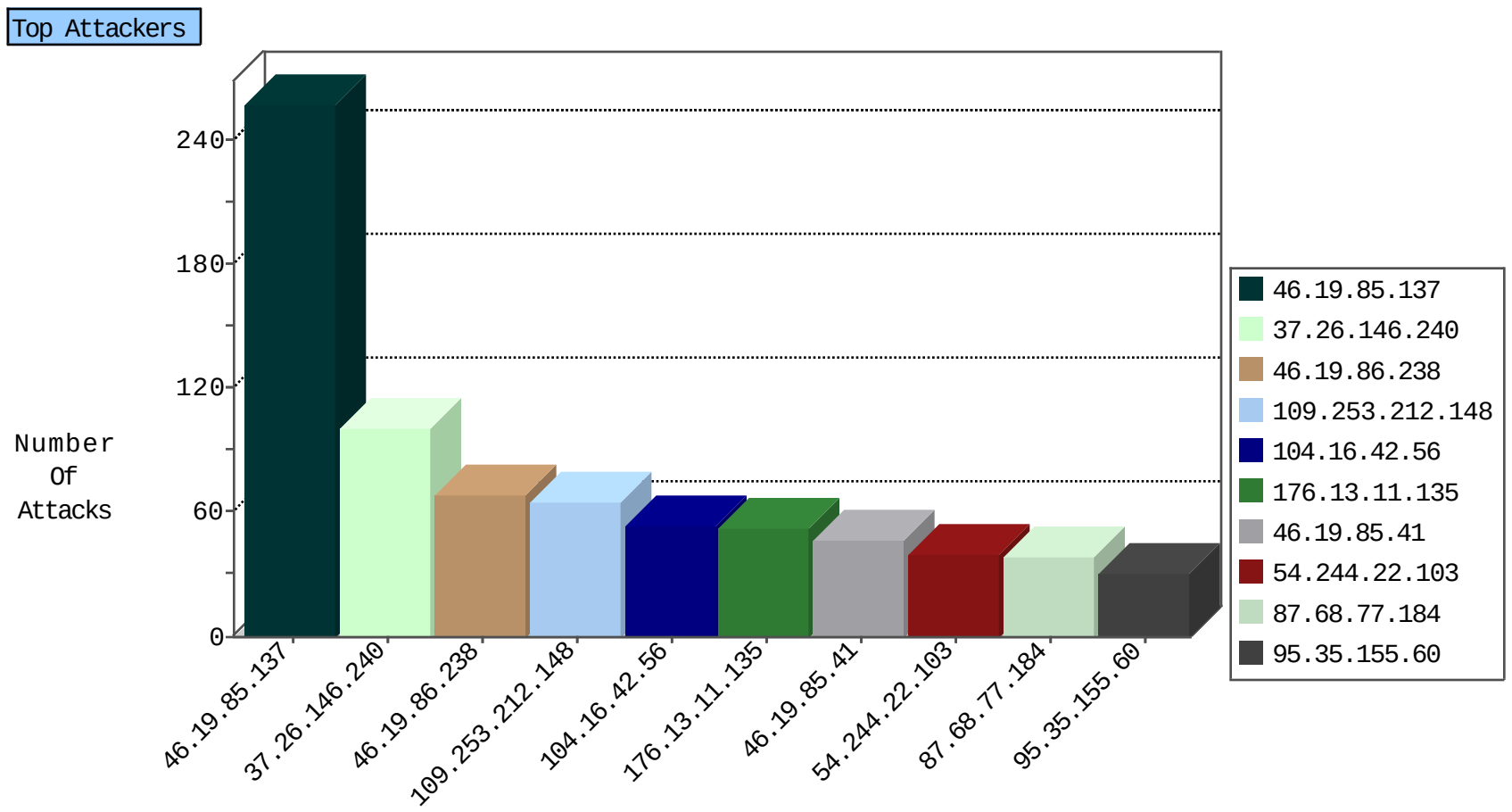
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-07-2016-12:04:07 to 02-07-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.77.184	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
213.8.241.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.13.10.189	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
107.191.42.168	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
123.195.107.68	Taiwan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

02-07-2016-12:04:07 to 02-07-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-12:04:07 to 02-07-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.28.155.17	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
193.254.206.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
79.176.163.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.66.209.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.168.218	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
89.138.196.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.74.123.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.115.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.230.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.164.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.128.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.230.93.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.168.218	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
89.139.170.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.57.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.206.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-12:04:07 to 02-07-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.41	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
104.16.42.56	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
104.16.42.56	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
95.35.155.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
176.13.16.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
87.68.77.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.176.201.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.0.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
84.229.29.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.222.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.11.135	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
95.35.155.60	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
62.0.222.1	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	7
80.246.139.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.177.223.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.151.32.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.108	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.43	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.39.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.216.233.24		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.5.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.144.64	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.213	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
87.69.205.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.10.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.181.228.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.10.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.20.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.212.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.112.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-07-2016-12:04:07 to 02-07-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.137	Block	109
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
109.253.212.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.137	Block	44
176.13.11.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
62.90.221.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.139.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.16.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.0.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
85.64.229.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
2.54.129.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.41.73	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
176.13.1.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
216.72.40.186	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1669-he/refuah.aspx	Block	2
85.64.229.107	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
79.177.223.64	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	2
213.8.125.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
46.19.85.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.78.67	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/894-he	Block	1
46.19.86.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.8.145.99	Israel	147.237.72.156	aman.idf.il	Multiple signatures from 213.8.145.99	Block	1
84.108.104.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/sachar	Block	1
37.26.146.168	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
79.176.166.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
141.212.122.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
93.157.85.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gios	Block	1
82.81.52.131	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$120 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.149.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.182.122.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.34.92	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
80.246.133.157	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
207.46.13.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
149.78.243.120	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
94.158.61.236	Uzbekistan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
62.219.122.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.235.53.213	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
82.102.227.115	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
31.13.110.117	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
79.183.189.240	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1012-en/eitan.aspx	None	1
109.66.37.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

02-07-2016-12:04:07 to 02-07-2016-13:04:07