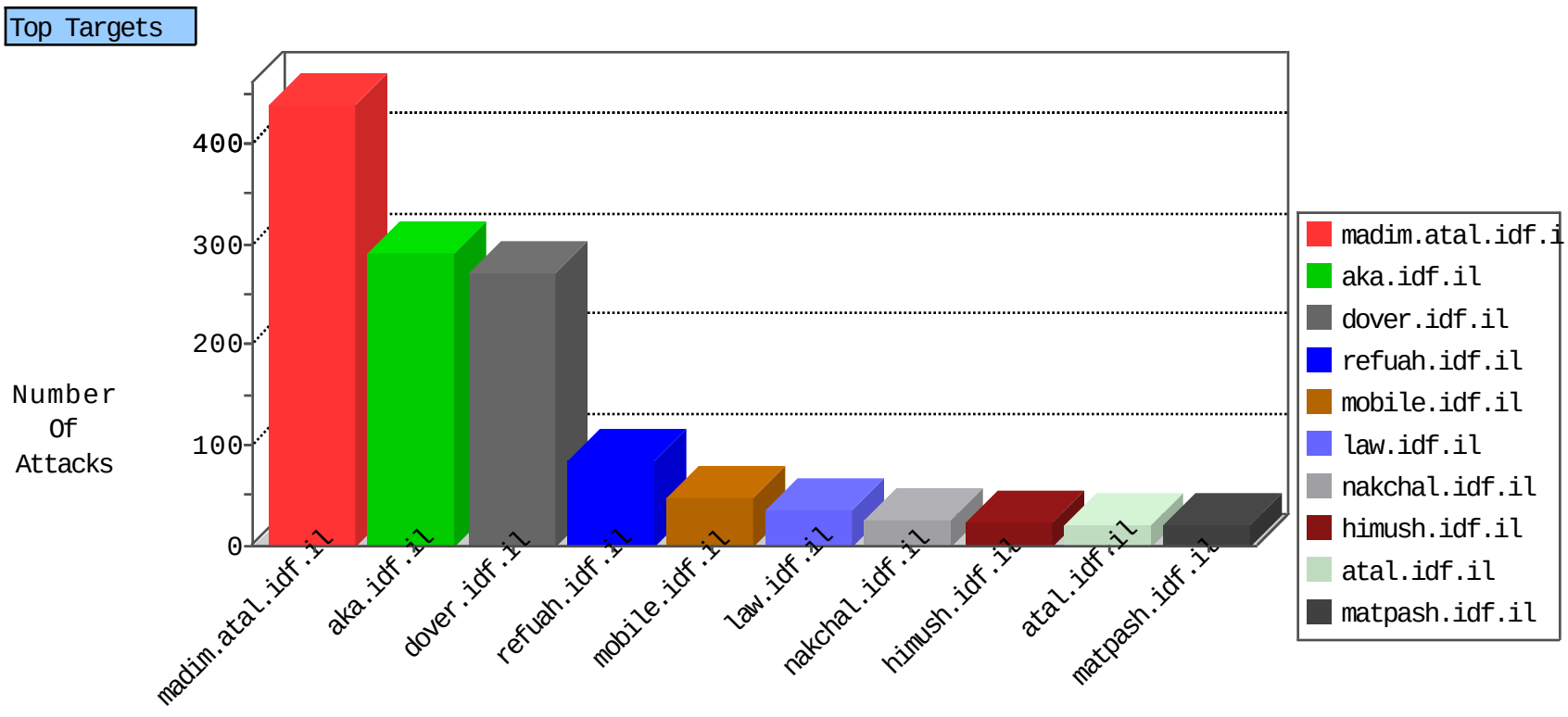
02-04-2016-14:04:04 to 02-04-2016-15:04:04

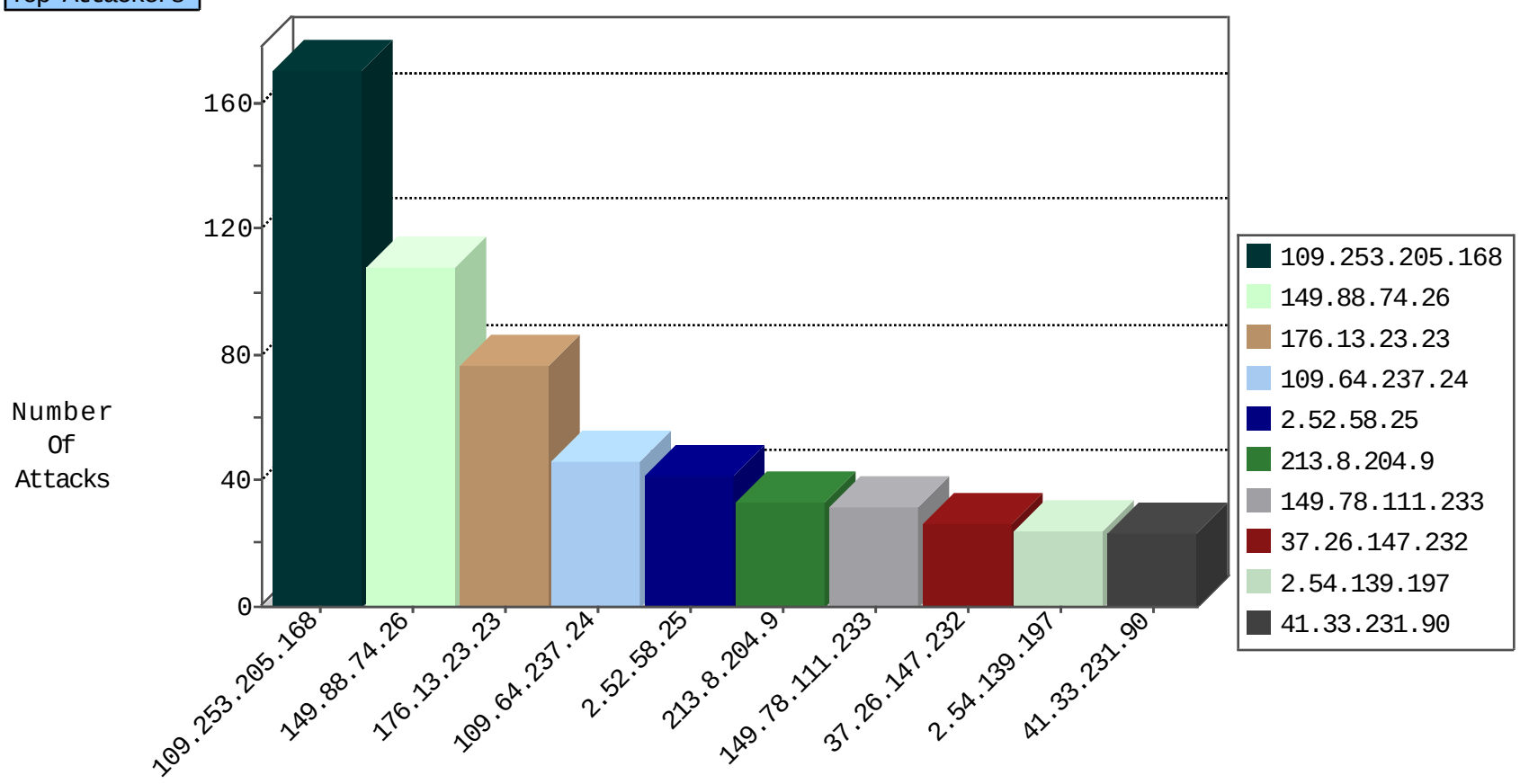
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-04-2016-14:04:04 to 02-04-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.122.252.41	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.72.166	aka.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1

02-04-2016-14:04:04 to 02-04-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.120.204.172	Israel	147.237.77.170	maarachot.idf.il	C008: HTTP: Xenu UserAgent	Block	1
46.120.204.172	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-04-2016-14:04:04 to 02-04-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.88.40.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.196	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.146.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.207	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.180.31.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.33.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.203.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
147.236.232.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.179.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.160.196	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.86.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.162.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.46.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-04-2016-14:04:04 to 02-04-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.237.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
2.52.58.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
149.78.111.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
2.54.139.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
213.57.127.178	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
80.246.130.207	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.203.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.20.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
165.225.72.85	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.130.207	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.52.10.200	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.198.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
62.0.197.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.198.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.169	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.143.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.165	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.170.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	6
2.54.173.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.218.173.126	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.148.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.169.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.146.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.168.17.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.9.122.202	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.132	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.56.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.146.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
73.3.77.56	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.38.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
149.78.40.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.228.194.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.60.144.32	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.169.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.8.204.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

02-04-2016-14:04:04 to 02-04-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
149.88.74.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.23.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
109.253.205.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
213.8.204.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
149.88.74.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.54.146.230	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 2.54.146.230	Block	14
5.28.137.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.253.205.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.205.168	Block	12
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.54.31.56	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	5
50.63.197.202	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.63.197.202	Block	5
46.19.86.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.137.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.148.175	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.148.175	Block	4
176.13.0.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.203.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.109.73.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	2
104.131.176.65	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.131.176.65	Block	2
5.22.131.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
194.90.25.122	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 194.90.25.122	Block	2
70.168.223.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
109.253.144.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.86.98.70	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.26.149.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
125.165.25.217	Indonesia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.248	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.80.194.30	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
37.26.148.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.186.4.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$108 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1362-he/dover.aspx parameter PageNum	Block	1
98.143.148.107	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/check	Block	1
85.64.17.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
50.63.197.202	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
84.94.73.177	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
37.190.185.123	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
2.54.158.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.187.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$43 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
77.126.82.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
191.232.136.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.88.74.26	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
132.64.165.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 132.64.165.89	Block	1
84.109.73.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.76.105.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1

02-04-2016-14:04:04 to 02-04-2016-15:04:04