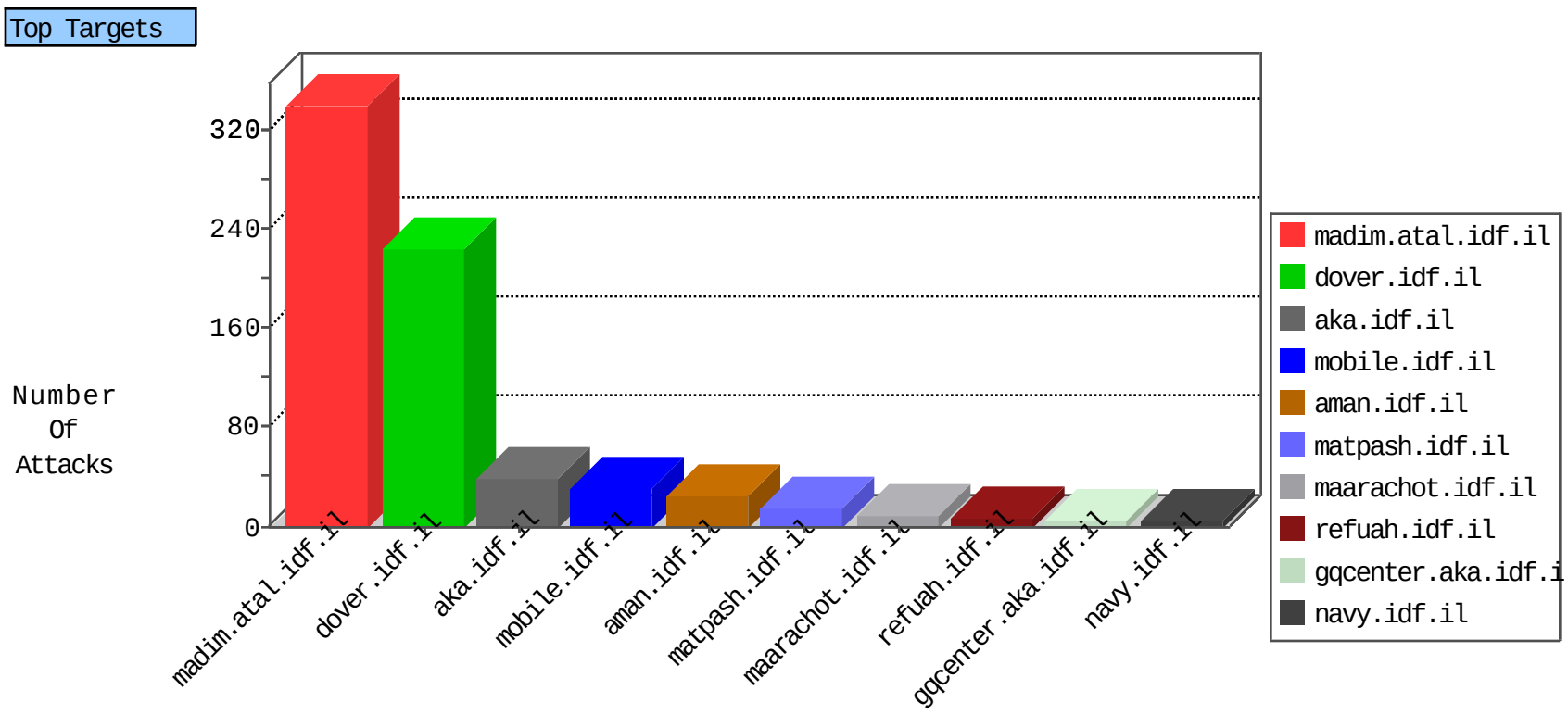
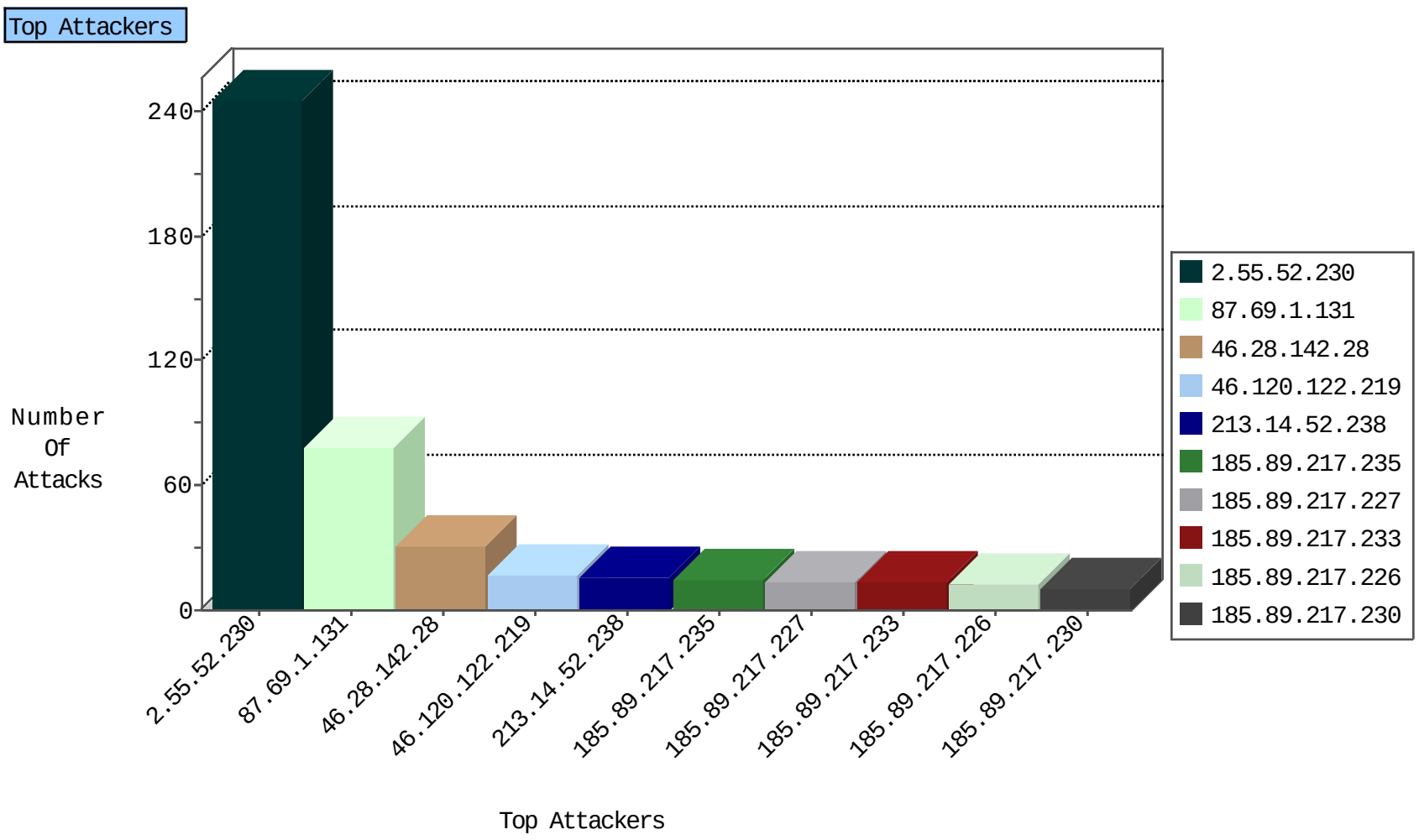
08-29-2016-20:04:09 to 08-29-2016-21:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-29-2016-20:04:09 to 08-29-2016-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.96.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
168.235.196.94	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.64.230.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
120.132.50.135	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1

08-29-2016-20:04:09 to 08-29-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6

08-29-2016-20:04:09 to 08-29-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.68.55.216	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
185.159.36.2	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
185.159.36.2	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	2
185.159.36.2	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	2
185.159.36.2	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1
112.217.150.112	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
112.217.150.112	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
97.105.173.114	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
185.159.36.2	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.76.42	Singapore	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
112.217.150.112	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.64.16.125	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
12.68.215.78	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.159.36.2	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.159.36.2	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1

08-29-2016-20:04:09 to 08-29-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.28.142.28	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.14.52.238	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.120.122.219	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	8
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.28.142.28	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.187.43.20	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.92.38.82		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	4
85.64.230.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.232.93	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.4	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
100.92.14.207		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.144	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
84.109.51.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.188.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
100.92.181.102		147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.74	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.147.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.11.180	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.220.76.76	Iceland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
123.184.18.133	China	147.237.0.33	idf.il	drop		drop	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
71.6.146.185	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.65.47.27	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
87.69.249.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.116.211.227	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.186	United States	147.237.0.200	m4u.idf.il	drop		drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.234.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1

08-29-2016-20:04:09 to 08-29-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.52.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	246
87.69.1.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
109.64.82.24	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
176.13.239.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
80.246.138.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
77.139.57.13	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
80.246.138.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
84.94.39.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/m/main/giyus/general.aspx	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.21.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.116.169.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.141.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.29.168.240	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.232.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.28.136.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
109.186.83.193	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.83.193	Block	1
79.176.106.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.240	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/smalim/showbig.aspx	None	1
46.19.86.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.139.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
80.246.137.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.243.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.45.87	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.102.9.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.186.83.193	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
84.94.82.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.85.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.192.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.204.52.13	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.116.13.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
176.13.244.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.102.9.118	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.5.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.192.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/sachar/forgotpassword.aspx	Block	1
77.139.106.92	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1

08-29-2016-20:04:09 to 08-29-2016-21:04:09