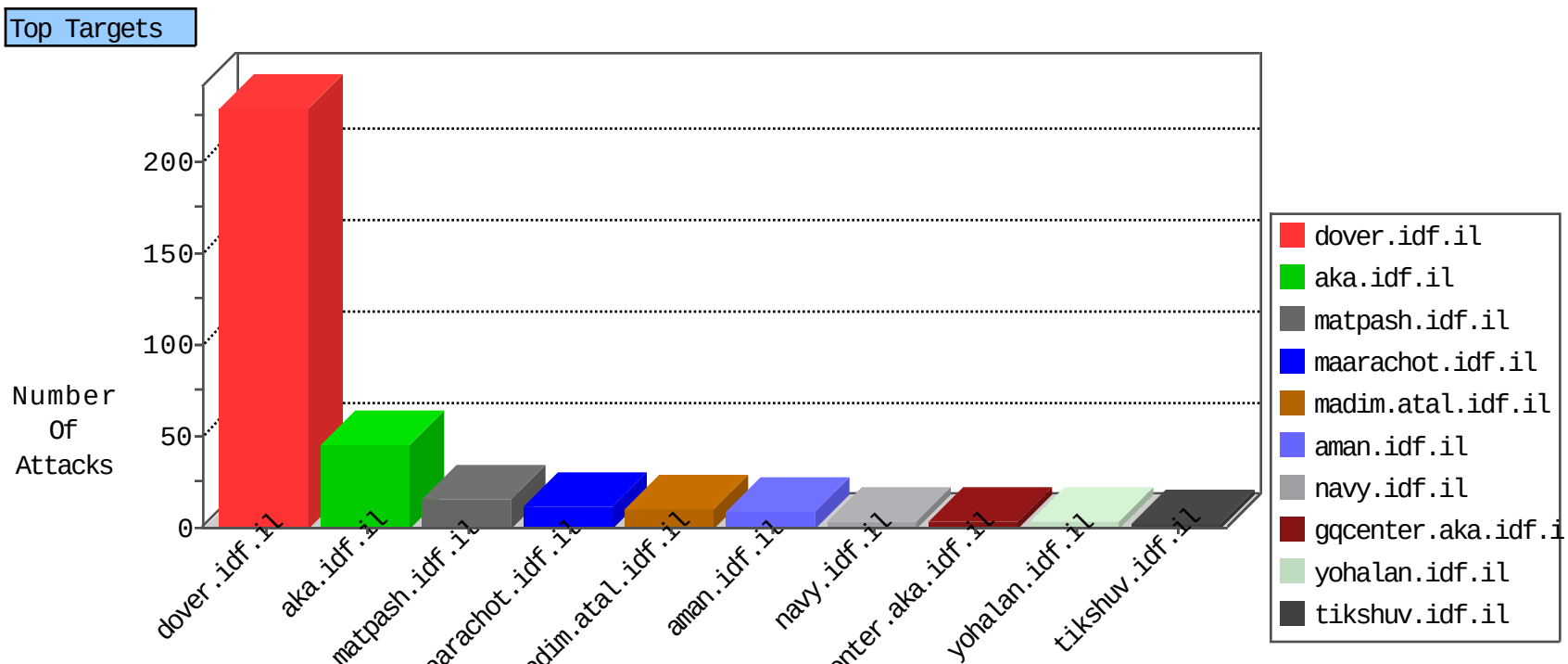
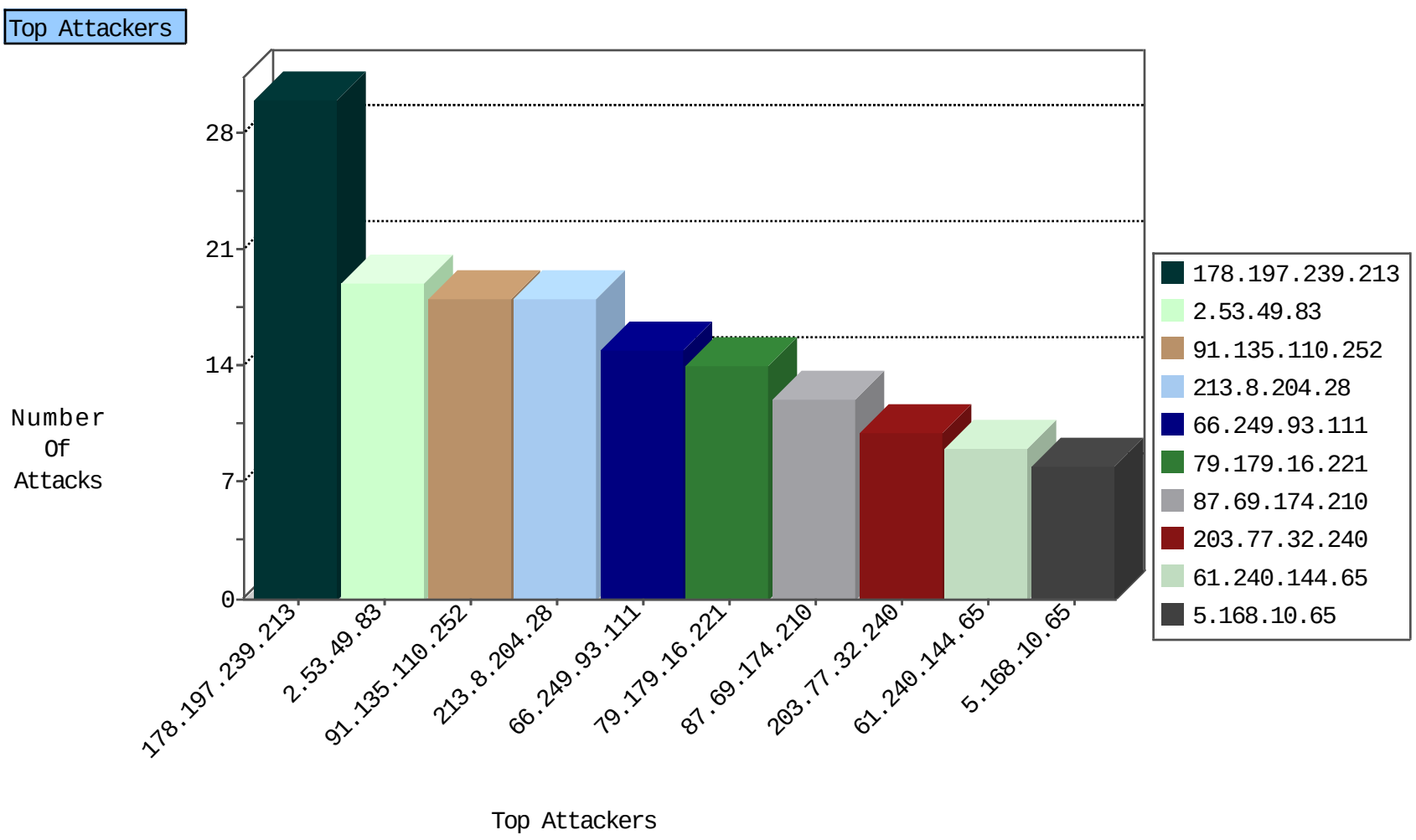
09-03-2016-22:04:08 to 09-03-2016-23:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-03-2016-22:04:08 to 09-03-2016-23:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.139.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
66.240.219.146	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

09-03-2016-22:04:08 to 09-03-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-22:04:08 to 09-03-2016-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.95.64	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
89.248.163.3	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.93.185	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.66	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.60.153.178	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.60.153.178	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.60.153.178	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.163.3	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.236.194.161	147.237.77.235	Czech Republic	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.226	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.253.209.191	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.240.144.65	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.60.153.178	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.60.153.178	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
104.128.144.131	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-03-2016-22:04:08 to 09-03-2016-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.197.239.213	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.53.49.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
91.135.110.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.8.204.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.179.16.221	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
87.69.174.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
203.77.32.240	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.168.10.65	Italy	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
85.250.101.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.32.208.95	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.167	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.185	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
177.86.1.194	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.179.38.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.8.204.28	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
79.179.153.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.56	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
46.19.85.89	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
5.29.128.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.200.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.177.235.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.239	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
31.146.14.189	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.205.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.146.75	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.29.175.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
87.71.29.74	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
46.43.104.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
84.108.147.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
89.139.108.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.219.137.5	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.202.7	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
85.65.203.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.178.100.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
213.8.204.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
81.218.106.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.10	Israel	147.237.0.33	idf.il	drop		drop	1
212.76.106.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
79.179.16.221	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1

09-03-2016-22:04:08 to 09-03-2016-23:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.199.85	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.199.85	Block	6
77.139.75.233	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
109.66.105.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.20	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
45.79.95.64	United States	147.237.77.170	maarachot.idf.il	Distributed Malformed URL	Block	2
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
45.79.95.64	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	2
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
62.219.137.5	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.206.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method szsd1r32qbnumlzfxn4 in URL	Block	1
23.234.19.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
85.219.205.227	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
62.0.102.190	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 62.0.102.190	Block	1
207.46.13.134	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.134	Block	1
109.64.190.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
46.19.85.36	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
79.180.9.224	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
151.213.145.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
77.138.54.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
62.0.102.190	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
207.46.13.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/dover.aspx-title=chief	Block	1
109.64.193.237	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.36	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method shuv.aspx in URL	Block	1
2.53.4.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.230.231.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl61 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/webservices/wscity.asmx	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
157.55.39.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.8.204.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
2.55.44.101	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.130.183	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.73.201	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/tizmoret/news/	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
89.138.174.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
45.79.95.64	United States	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 4	Block	1
77.139.85.133	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.102.9.98	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
23.234.19.163	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.108.240.59	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.108.240.59	Block	1
66.249.79.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
188.120.132.242	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
109.64.190.196	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.190.196	Block	1
45.79.95.64	United States	147.237.77.170	maarachot.idf.il	Multiple Malformed HTTP Header Line from 45.79.95.64	Block	1

09-03-2016-22:04:08 to 09-03-2016-23:04:08