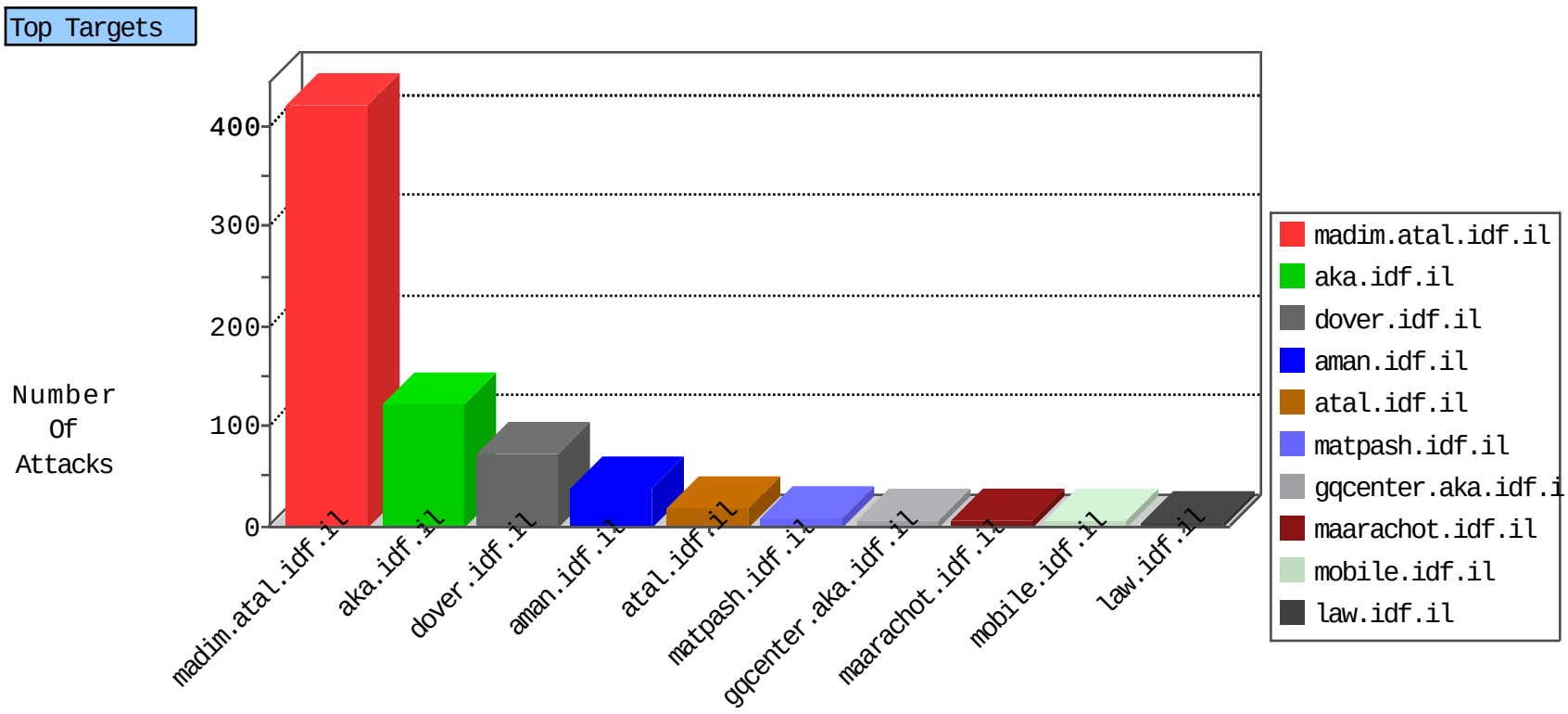
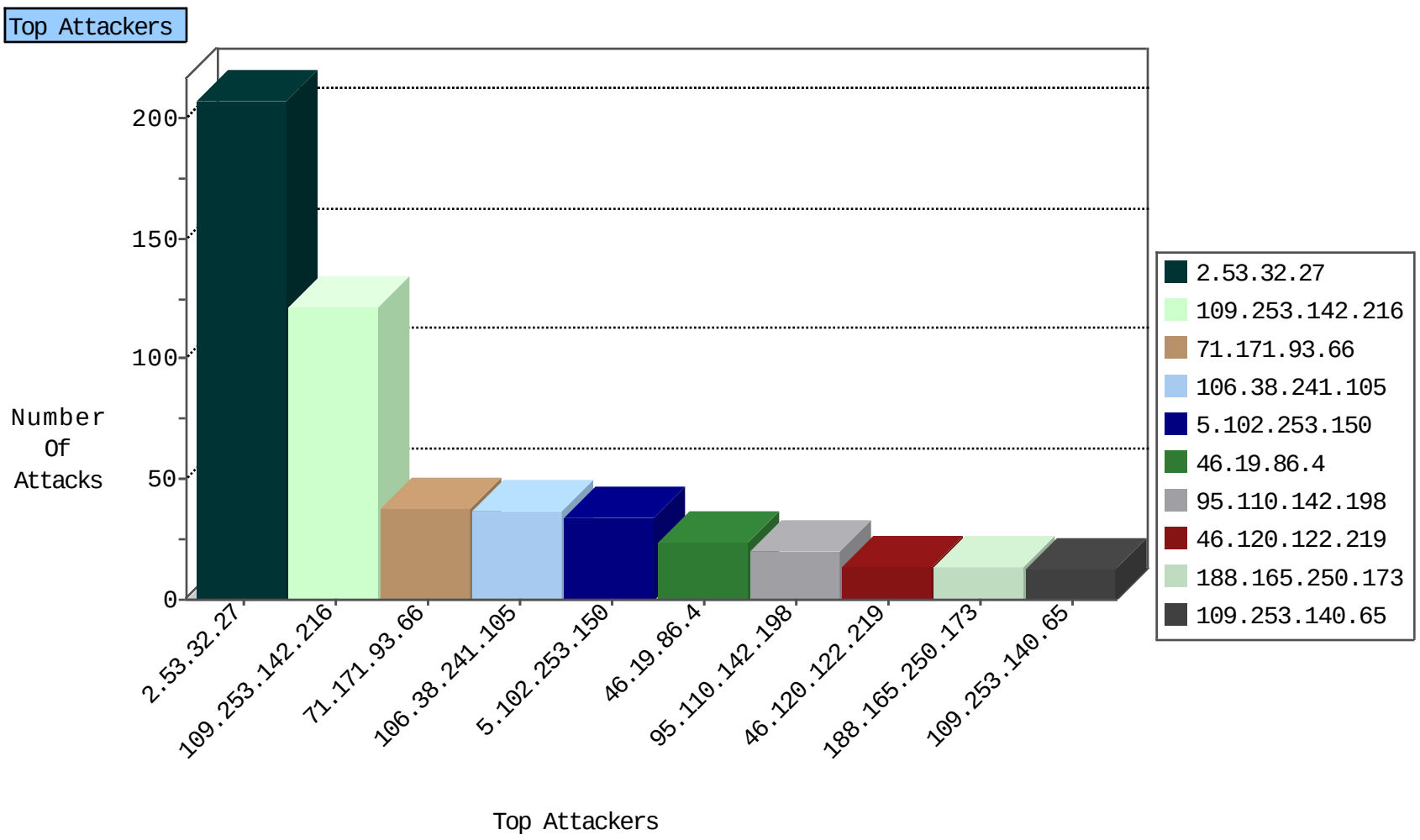
08-29-2016-22:04:09 to 08-29-2016-23:04:09

IDF Under Attack
Daily Report





08-29-2016-22:04:09 to 08-29-2016-23:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1

08-29-2016-22:04:09 to 08-29-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	19
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	13
71.171.93.66	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
95.110.142.198	Italy	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
188.165.250.173	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.171.93.66	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
95.110.142.198	Italy	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-29-2016-22:04:09 to 08-29-2016-23:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
71.171.93.66	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	20
95.110.142.198	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	12
188.165.250.173	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
50.116.123.135	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.167.138	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.66.176.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.76.42	Czech Republic	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
210.73.208.201	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.139.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.77.74	Czech Republic	law.idf.il	ET SCAN NMAP -sS window 1024	1

08-29-2016-22:04:09 to 08-29-2016-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.92.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.55.188.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
173.208.194.114	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
176.13.241.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	5
46.120.122.219	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
109.65.88.61	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
109.253.210.56	Israel	147.237.72.166	aka.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
199.30.80.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.218.112	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.7.236	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.179.58.249	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.0.125	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
2.53.149.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.13	Israel	147.237.0.33	idf.il	drop		drop	1
176.13.241.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.160.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
109.253.141.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.120.122.219	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
185.120.125.115	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.21.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.147	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
61.240.144.65	China	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
176.13.224.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-29-2016-22:04:09 to 08-29-2016-23:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.32.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	208
109.253.142.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
5.102.253.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
109.253.140.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
84.111.104.32	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
2.53.174.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
89.139.174.127	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
216.81.94.72	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	4
84.94.40.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.174.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
181.67.103.228	Peru	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/klali/default.asp	Block	3
82.81.81.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.139.168.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.56.184	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.56.184	Block	2
68.101.233.221	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	2
85.64.165.209	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
99.31.227.98	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
176.13.234.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
192.116.190.42	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights	Block	1
131.253.27.80	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
2.53.56.184	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
212.76.122.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
163.172.138.81	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 163.172.138.81	Block	1
109.186.86.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
85.64.165.209	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.165.209	Block	1
79.180.60.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
141.226.217.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/900-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
84.108.125.170	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.125.170	Block	1
176.13.13.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.155.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13606-he/dover.aspx„'"•'×' ƒ„'„†λ€™„ƒλ€š„,„¯„ƒ„'„¢λ,¬„¡„ƒλ€š„,„¿„ƒ„'„¢λ,¬„¡„ƒλ€š„,„½	Block	1
157.55.39.1	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.108.125.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	1
76.79.189.147	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.65.20.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
207.46.13.148	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/scripts.asmx/getjs	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1

08-29-2016-22:04:09 to 08-29-2016-23:04:09