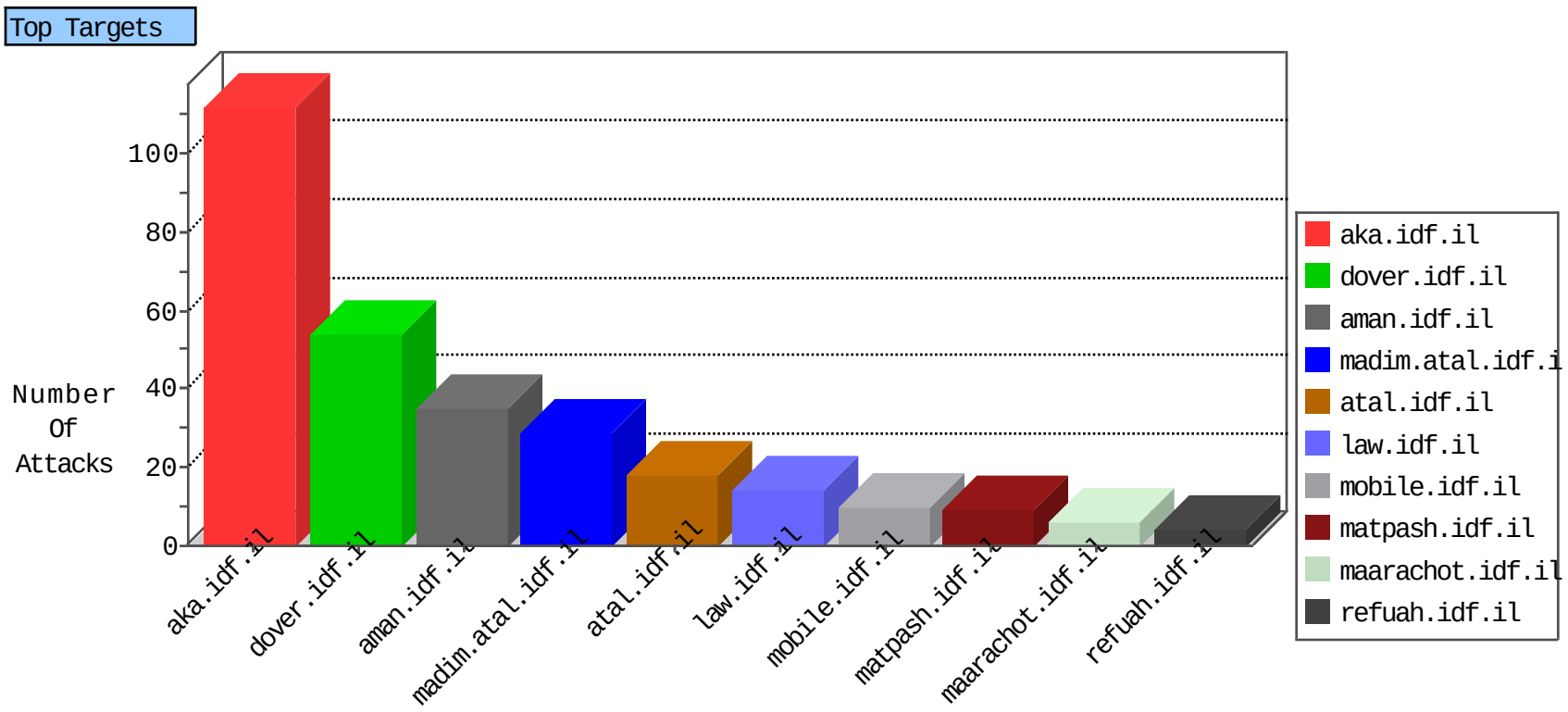
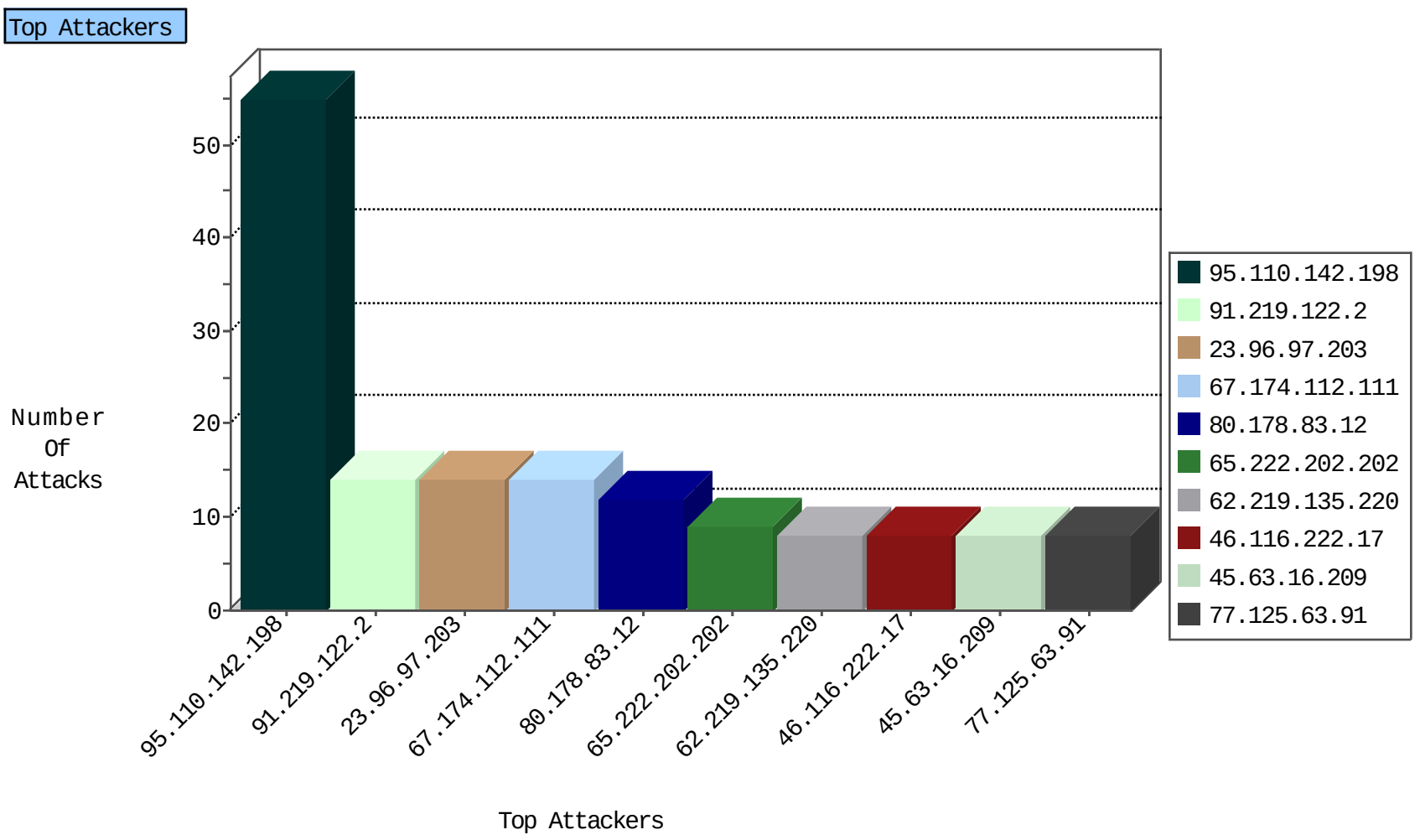
08-29-2016-21:04:00 to 08-29-2016-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-29-2016-21:04:00 to 08-29-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.124	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
220.181.167.182	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
209.126.136.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
2.53.144.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.138.102.144	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
45.55.219.114	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	Black List	drop	1
45.55.219.114	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

08-29-2016-21:04:00 to 08-29-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.110.142.198	Italy	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
23.96.97.203	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
67.174.112.111	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
95.110.142.198	Italy	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

08-29-2016-21:04:00 to 08-29-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.110.142.198	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	44
23.96.97.203	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
67.174.112.111	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
91.219.122.2	147.237.77.233	Poland	atal.idf.il	SQL Injection - Select From	8
77.125.63.91	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
77.125.63.91	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
45.63.16.209	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
97.105.173.114	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.209	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.50.45	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.102.9.167	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
45.63.16.209	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
220.181.167.182	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
45.63.16.209	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
198.167.223.33	147.237.76.38	Saint Kitts and Nevis	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.209	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.209	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
37.142.219.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.172.71.251	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.209	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
217.118.23.124	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.16.209	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
168.235.196.94	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

08-29-2016-21:04:00 to 08-29-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.219.135.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.232.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.116.222.17	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
176.67.104.90	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.120.122.219	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
46.117.97.134	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
176.13.0.100	Israel	147.237.77.216	dover.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
37.46.38.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.211.20	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.227.235	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.121.182	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
100.92.180.7		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
109.253.192.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.120.124.44	Israel	147.237.77.216	dover.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
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
109.253.212.104	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.181	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.249.81.183	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
176.13.248.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.83.12	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
65.222.202.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
77.138.205.170	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/viewpayslip.aspx	Block	6
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.89.225	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
176.13.241.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.6.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	3
65.222.202.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.157.22	France	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.235.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	2
62.219.92.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.143.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.149.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
71.190.221.51	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
65.222.202.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.234.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.235.21	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.235.21	Block	2
109.65.15.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
87.71.1.198	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
220.255.183.170	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	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
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.122	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
89.138.160.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/w	Block	1
46.31.97.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
109.253.141.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.229.27.98	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
77.138.243.99	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
192.211.49.200	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.57	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
89.237.70.83	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.31.160.45	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim	Block	1
5.102.195.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.172.240	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
77.125.63.91	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.63.91	Block	1
176.228.24.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/112450.pdf	Block	1
85.64.255.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.85.169	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.139.152.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.249.66.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
46.116.49.187	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1