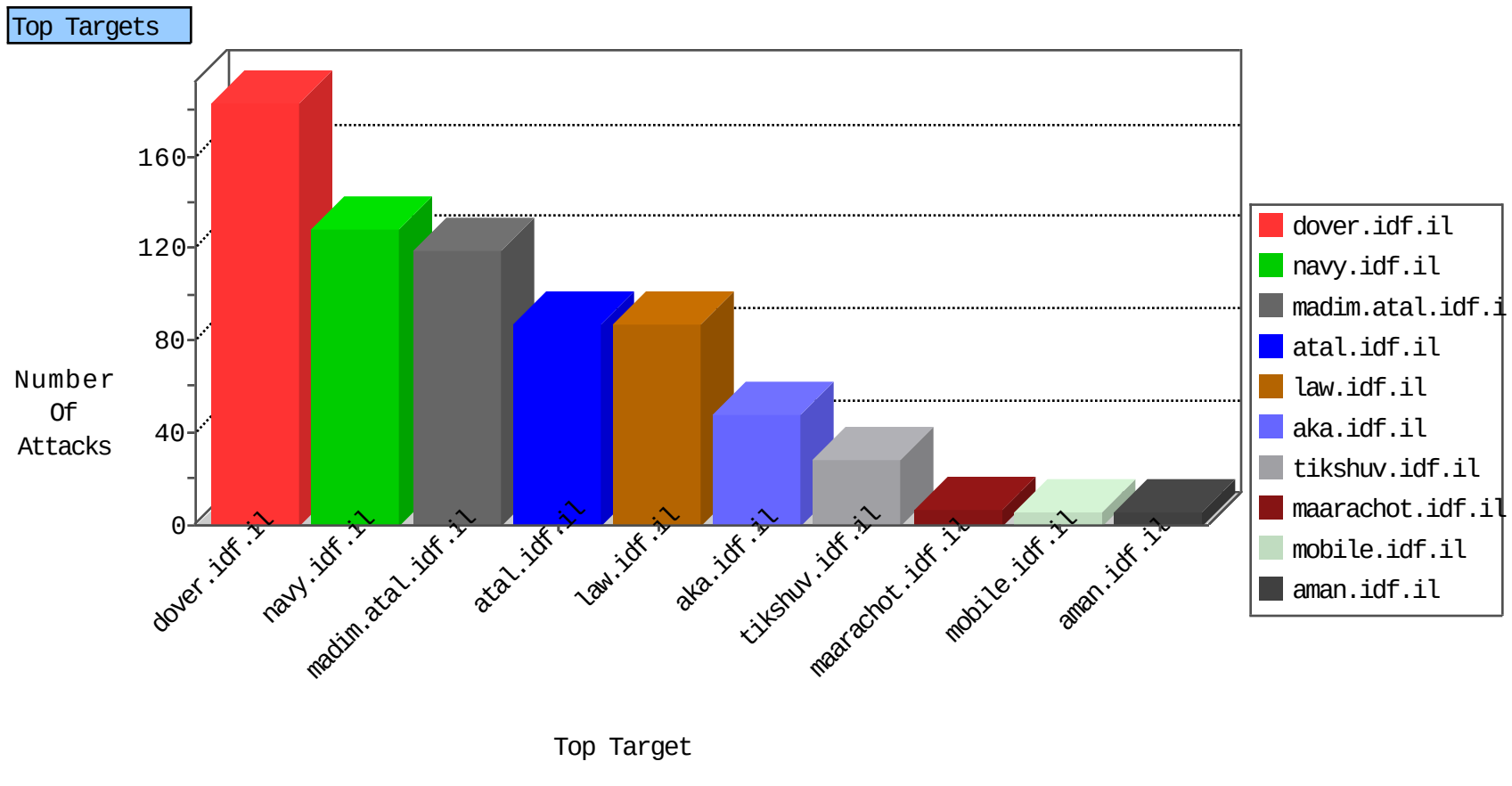
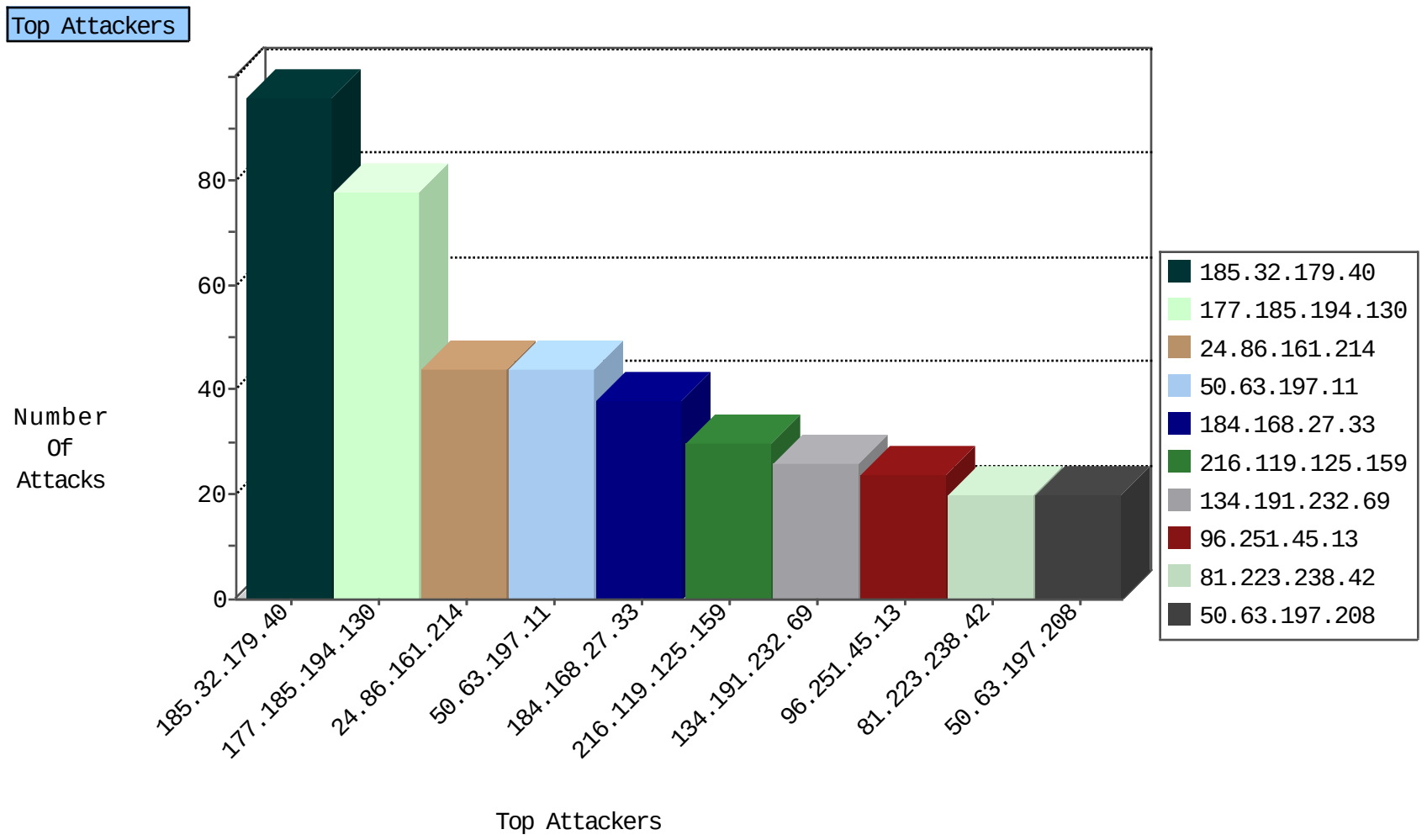
08-24-2016-17:04:01 to 08-24-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-24-2016-17:04:01 to 08-24-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.0.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
50.84.0.150	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
212.199.34.114	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
95.111.129.119	Ukraine	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
2.53.32.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
95.111.129.119	Ukraine	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
50.84.0.150	United States	147.237.72.14	dover.idf.il(old)	JLM_Purple_Con_Limit_Tcp	drop	1

08-24-2016-17:04:01 to 08-24-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.63.197.11	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.27.33	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
24.86.161.214	Canada	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.180.89.124	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.130	Brazil	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
195.74.38.15	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.11	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
128.187.112.4	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.33	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
96.251.45.13	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.86.161.214	Canada	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.208	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.86.161.214	Canada	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.130	Brazil	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.223.238.42	Austria	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
121.40.25.174	China	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
205.144.171.34	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
178.20.235.164	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
121.40.25.174	China	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
213.115.226.16	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
185.100.87.139	Finland	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
83.64.189.179	Austria	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.126.68.138	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
205.144.171.34	United States	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
177.185.194.130	Brazil	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

08-24-2016-17:04:01 to 08-24-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.194.130	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	52
50.63.197.11	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	26
24.86.161.214	147.237.76.86	Canada	navy.idf.il	SQL Injection - Select From	26
216.119.125.159	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	24
184.168.27.33	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
96.251.45.13	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	18
81.223.238.42	147.237.77.233	Austria	atal.idf.il	SQL Injection - Select From	15
50.63.197.208	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	14
213.180.89.124	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	13
195.74.38.15	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	8
178.20.235.164	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
128.187.112.4	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
121.40.25.174	147.237.77.233	China	atal.idf.il	SQL Injection - Select From	5
177.185.194.130	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	4
177.185.194.130	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	4
83.64.189.179	147.237.77.233	Austria	atal.idf.il	SQL Injection - Select From	3
205.144.171.34	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	1
202.83.21.48	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.52.97	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
31.223.176.126	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.76.147	Japan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.80.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
203.4.240.101	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 3072	1
201.238.202.219	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.13.193.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.20.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.104.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.3.168	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

08-24-2016-17:04:01 to 08-24-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
134.191.232.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
94.136.40.77	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
109.253.142.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
177.185.194.130	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.145.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
193.43.246.250	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
2.55.12.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.120.206.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
176.13.250.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
37.142.239.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
94.197.120.108	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.66.0.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.32.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.32.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.203.130.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.135.199	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.34	United States	147.237.0.200	m4u.idf.il	drop		drop	1
203.133.169.169	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.251.60	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.40.0.13	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.227.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.232.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.248.203	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.67.200.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
148.251.2.180	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-24-2016-17:04:01 to 08-24-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
37.26.146.241	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	5
37.26.149.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.67.199.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.13.51	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
2.53.11.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.133.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.166.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.125.66.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.225.100	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.69.253	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	2
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
77.138.153.132	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.66.15	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation catId in www.navy.idf.il/navy/general.aspx	Block	1
80.230.225.138	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	1
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	1
46.229.164.99	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/patzar/news/default.asp	Block	1
84.95.255.154	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/108971.pdf	Block	1
2.84.56.219	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.69.194	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
131.253.25.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.230.225.140	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
66.102.9.54	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
85.26.232.208	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.181.59.232	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.127	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.225.198	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
89.139.236.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.83.12	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.69.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.116.136.164	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.133.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.30.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.50.50	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** **********, Observed ********** ********** **********	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1

08-24-2016-17:04:01 to 08-24-2016-18:04:01