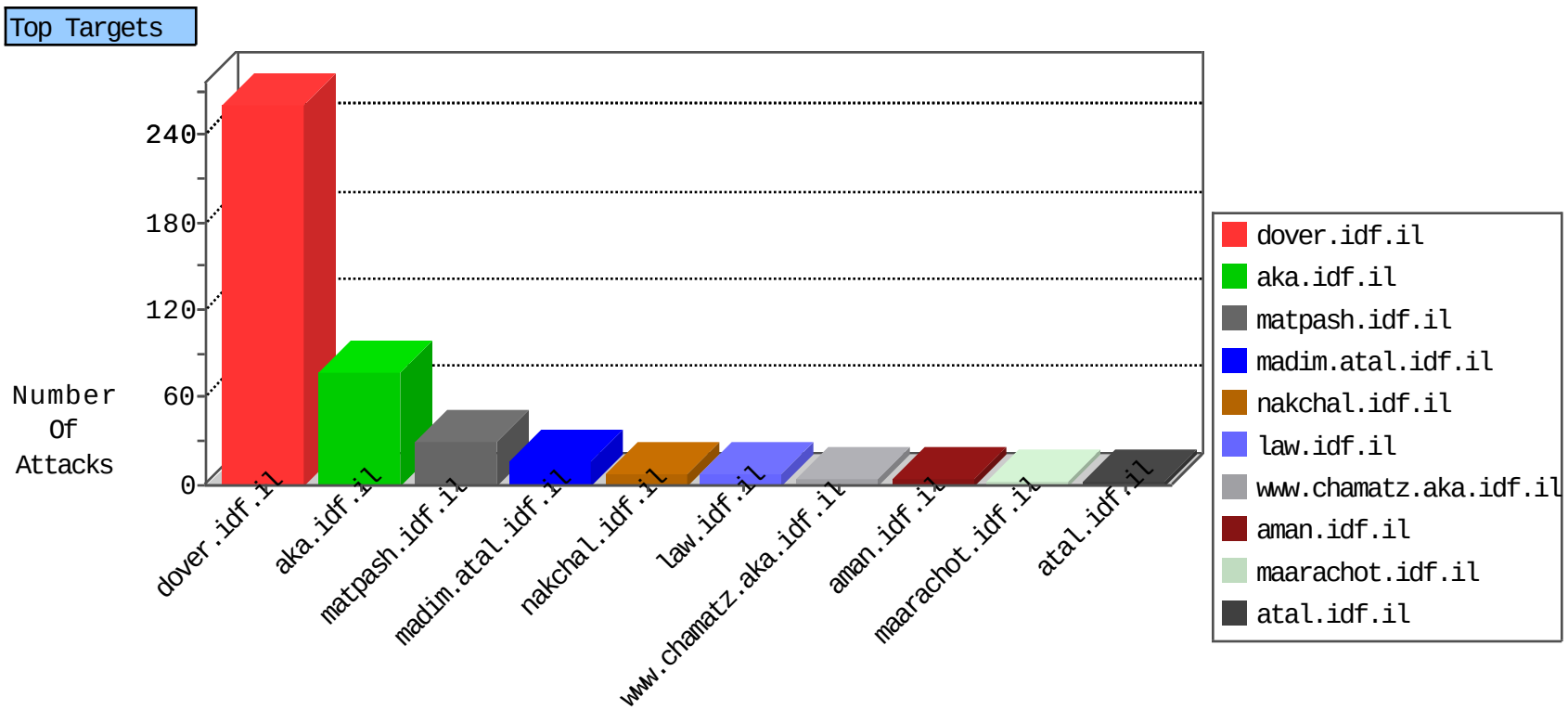
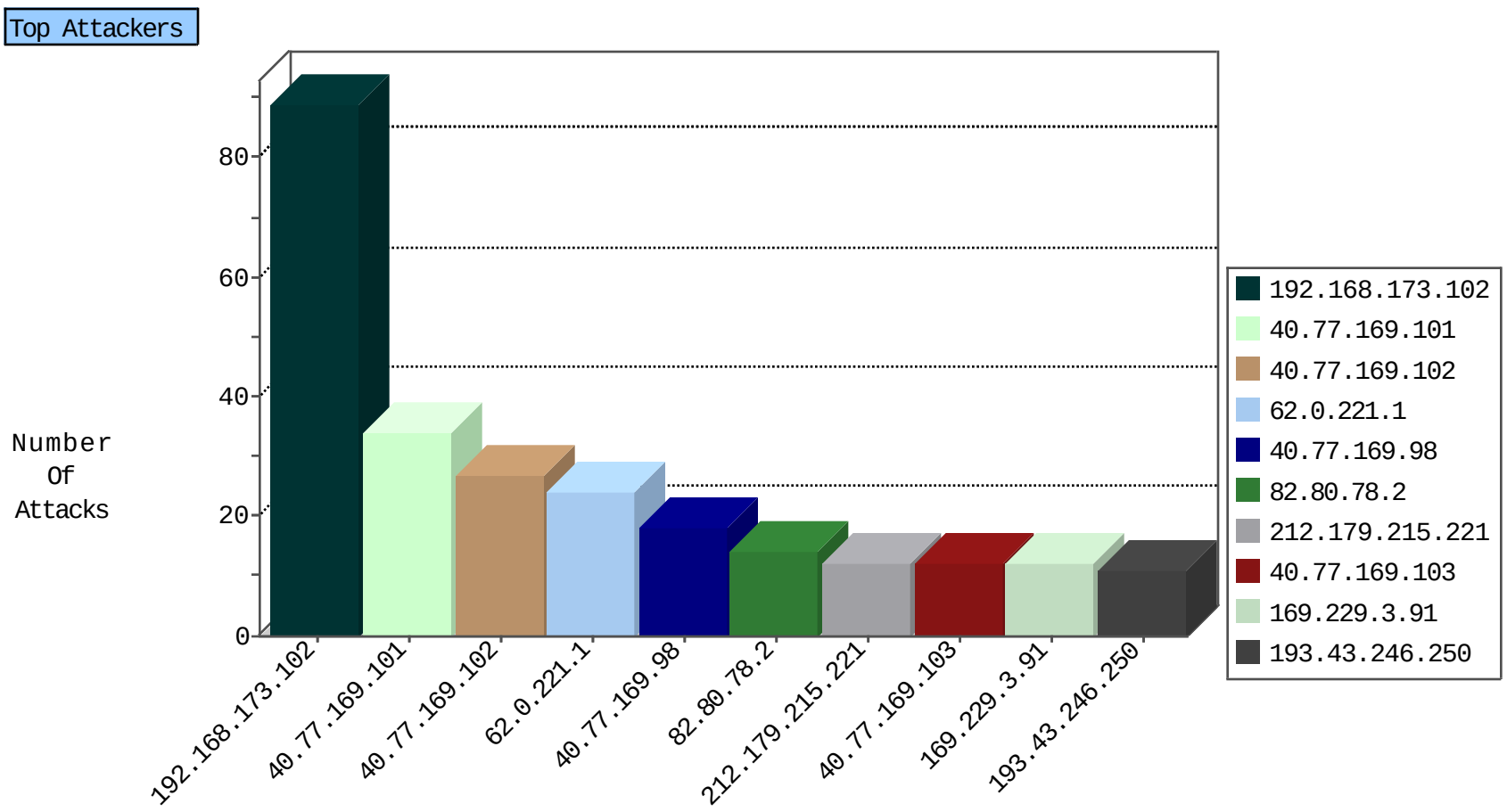
08-25-2016-13:04:05 to 08-25-2016-14:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-13:04:05 to 08-25-2016-14:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	14
93.158.200.166	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
212.199.130.50	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-25-2016-13:04:05 to 08-25-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-25-2016-13:04:05 to 08-25-2016-14:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.65.132.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
117.27.240.24	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
213.57.80.98	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	1
89.138.13.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.33.99.4	147.237.77.74	Palestinian Territory, Occupied	law.idf.il	ET SCAN NMAP -sA (2)	1
87.236.194.161	147.237.0.35	Czech Republic	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
85.64.62.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.248.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.56.80.144	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.114.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.127.121.73	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.100.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.8.24	Japan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.174.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.77.216	Japan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.130.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.13	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
109.67.219.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.63.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.236.194.161	147.237.76.44	Czech Republic	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
207.232.46.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.130.251.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
186.121.38.20	147.237.76.39	Colombia	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.182.146.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.106.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.8.27	Japan	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.95.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
133.242.3.168	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.135.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.13	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

08-25-2016-13:04:05 to 08-25-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	89
62.0.221.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	16
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
37.231.101.90	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.81.233	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
176.13.251.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.215.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
62.0.238.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
194.90.129.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
212.179.215.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.155.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.179.215.221	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
40.77.169.98	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.53	Israel	147.237.76.30	himush.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
176.13.246.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.97	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
74.82.47.58	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.95	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.17.36	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	SAM rule	drop	1
78.46.42.235	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.206	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
169.54.233.119	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
209.88.157.240	Israel	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.235.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
109.253.144.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.245.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-13:04:05 to 08-25-2016-14:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.203.203.50	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
37.142.9.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.109.202.86	Block	3
2.55.158.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
88.202.218.233	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.132.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.142.185	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
176.13.241.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.199.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.224.81	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
176.13.244.84	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.176.133.22	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 193.34.57.101	Block	2
77.139.5.154	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	2
185.32.179.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.179.163.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
83.220.239.122	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
204.79.180.23	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/portalmiluim/templates/inner.asp	Block	1
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
85.64.62.75	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
213.57.9.24	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.176.117.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
89.139.191.118	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
85.65.48.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.133.22	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.160	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
193.34.57.101	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
209.88.157.240	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
40.77.169.98	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /592-4071-en/patzar.aspx#011200	Block	1
87.69.172.182	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
2.53.145.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
209.88.157.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
87.71.34.117	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/funeral.stm israel defense forces' footage of the fake burial in jenin	Block	1
84.229.79.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
212.25.79.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.139.188.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.198.151.43	Block	1

08-25-2016-13:04:05 to 08-25-2016-14:04:05