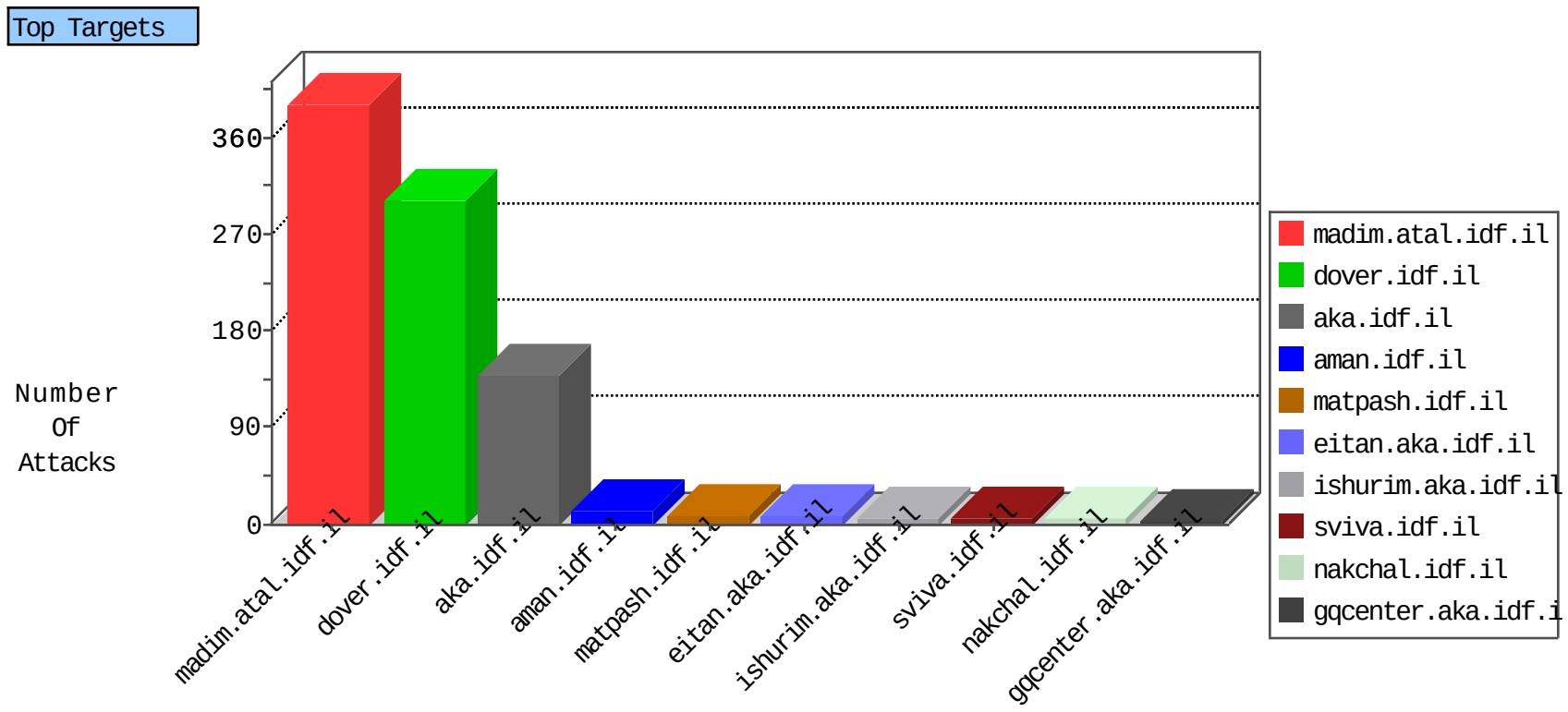
08-23-2016-16:04:04 to 08-23-2016-17:04:04

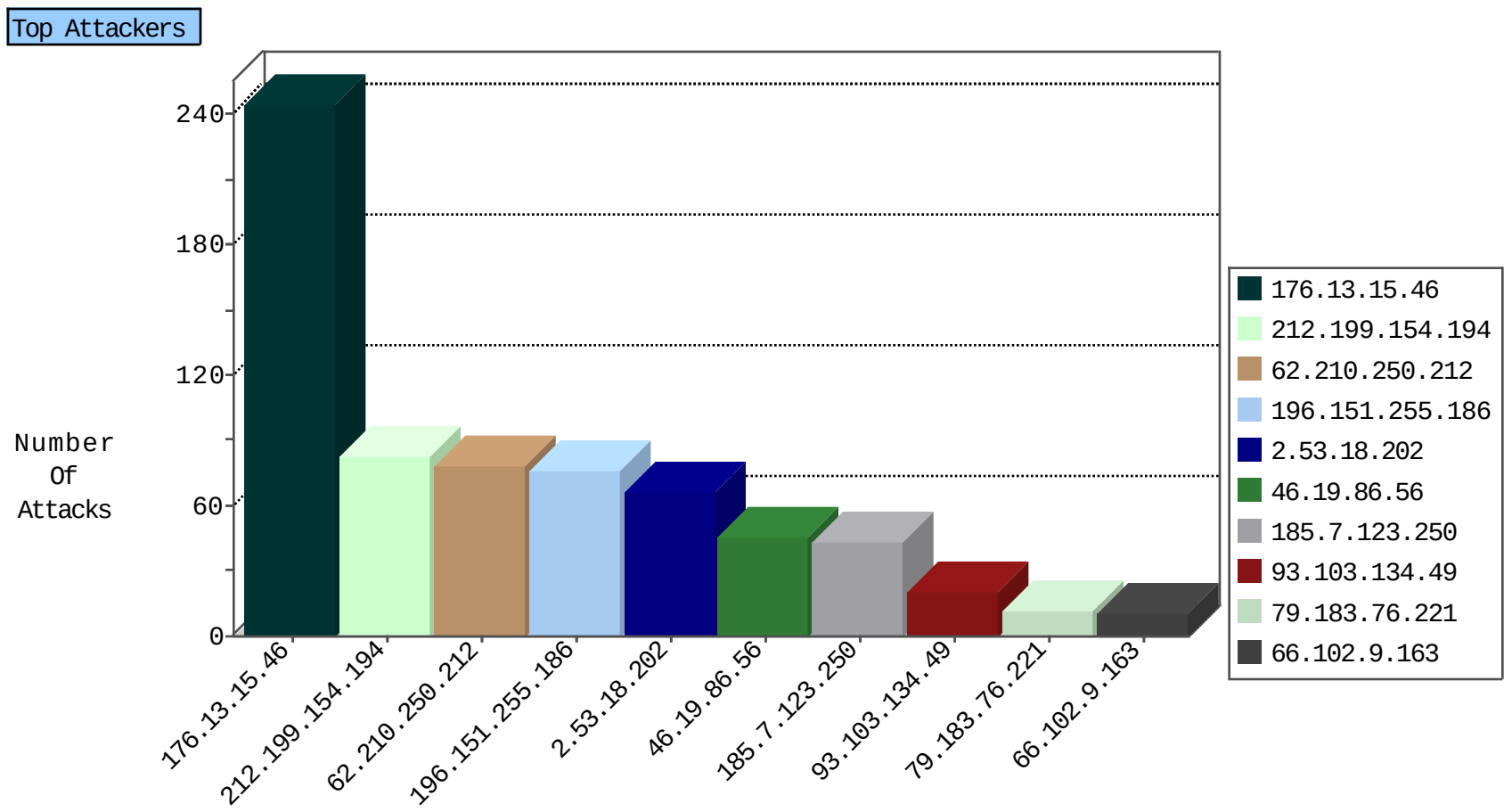
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-23-2016-16:04:04 to 08-23-2016-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	467
79.183.76.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
2.55.3.0	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
196.151.255.186	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
46.19.86.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.15.46	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
195.68.204.4	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.199.119.51	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-23-2016-16:04:04 to 08-23-2016-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.250.212	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	59
62.210.250.212	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	12
62.210.250.212	France	147.237.76.200	eitan.aka.idf.i	C1000074: HTTP: majestic bot	Permit	7
81.214.8.252	Turkey	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	1
52.32.172.31	United States	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
81.214.8.252	Turkey	147.237.77.233	atal.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

08-23-2016-16:04:04 to 08-23-2016-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.65.83.83	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
87.236.194.161	147.237.77.235	Czech Republic	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.209.182	147.237.77.234	Chile	halag.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -f -sS	1
82.81.218.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.181.171.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.200.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.15.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.123.119.180	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.75	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
123.123.119.180	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.195.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.228.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
202.155.58.28	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.36.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.171.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.2.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.204.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.165.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.123.119.180	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.83.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.123.119.180	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.219.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.38.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.91.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.228.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
207.241.225.244	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

08-23-2016-16:04:04 to 08-23-2016-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.151.255.186	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
185.7.123.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
93.103.134.49	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.102.9.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.114.174.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.117.182.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
212.179.214.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
89.138.137.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
185.7.123.250	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
176.13.225.179	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
147.123.249.9	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.76.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.68.204.4	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.150.78.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.220.50	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
197.119.80.251	Algeria	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.81.218	Europe	147.237.77.216	dover.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
46.255.84.17	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.13.113.80	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
176.13.23.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.216.116	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.237.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.66	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
31.13.113.94	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
192.243.55.137	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
141.212.122.79	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
176.13.225.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
176.13.226.106	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.64	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
5.22.132.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
176.13.3.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.206.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.234.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-16:04:04 to 08-23-2016-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	236
2.53.18.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
185.32.179.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.17.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.155.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
174.139.43.45	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 174.139.43.45	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.26.146.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.225.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.244.101	Israel	147.237.0.19	madim.atal.idf.il	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
84.109.69.113	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
109.253.140.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.157.111	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	2
93.173.45.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
79.181.174.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.64.181.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.181.95	Block	1
213.57.218.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gayus	Block	1
123.125.71.110	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
81.218.57.234	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	1
37.46.38.215	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.46.38.215	Block	1
109.64.181.95	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
67.63.160.38	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
157.55.39.132	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
37.46.38.215	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
109.66.1.10	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.124.47.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/gius	Block	1
46.117.167.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
84.109.69.113	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.0.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.102.9.184	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
174.139.43.45	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1

08-23-2016-16:04:04 to 08-23-2016-17:04:04