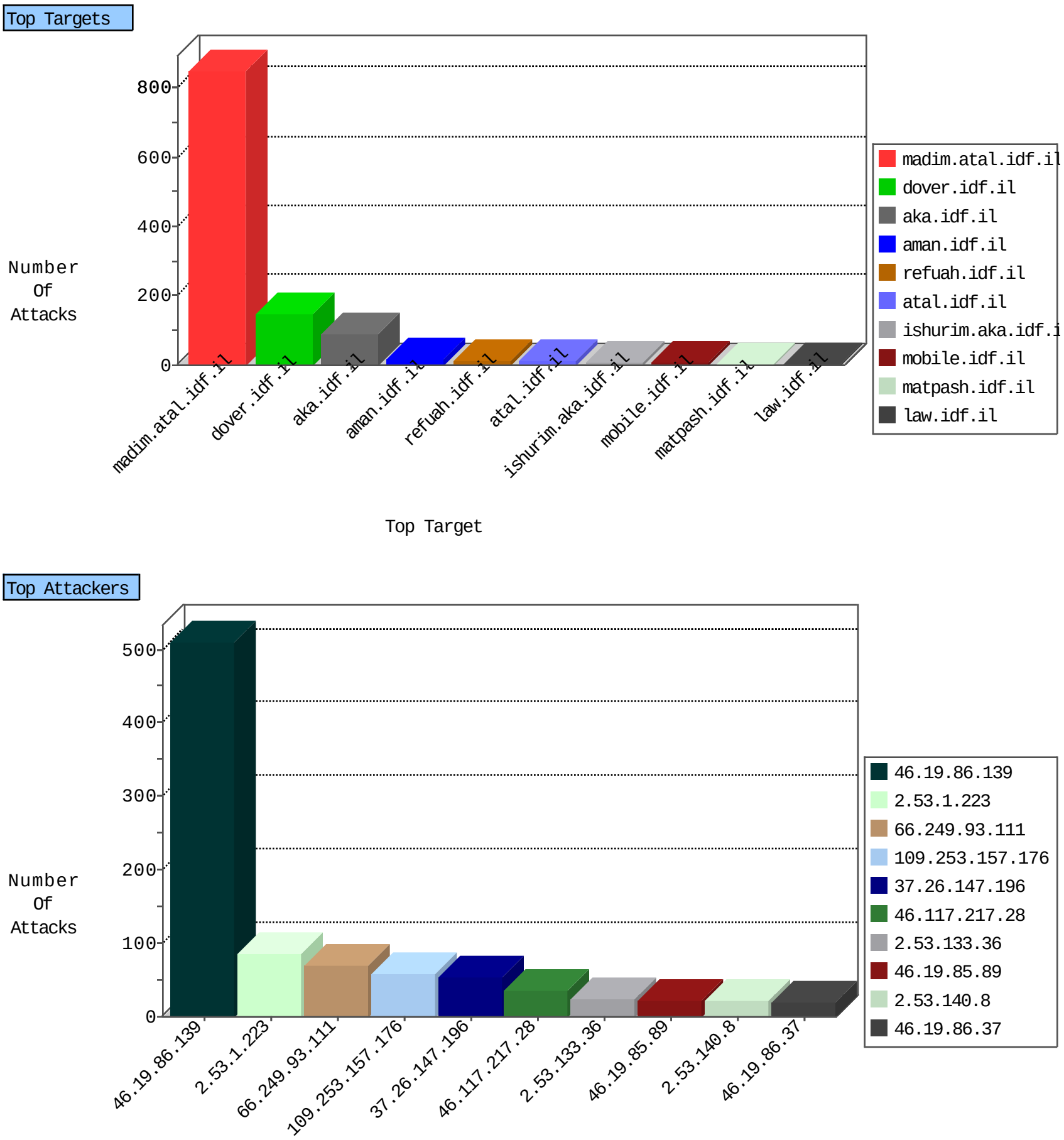
09-04-2016-09:04:07 to 09-04-2016-10:04:07

IDF Under Attack Daily Report



09-04-2016-09:04:07 to 09-04-2016-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
82.80.217.70	Israel	147.237.77.74	law.idf.il	Black List	drop	2
69.64.43.122	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
80.82.65.168	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-04-2016-09:04:07 to 09-04-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-09:04:07 to 09-04-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.11.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.135	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
217.132.126.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.117.176.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.212.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.178.143.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.113.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.78.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.50.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.197.206.193	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
37.26.148.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.135	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
194.90.129.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.237.118.247	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.12.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.66.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.251.236.237	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.35.162	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	1
109.66.113.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.206.193	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
37.46.35.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.135	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.197.206.193	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1

09-04-2016-09:04:07 to 09-04-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	64
46.117.217.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	35
46.19.85.89	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	22
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.243	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	11
46.19.85.239	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
46.19.86.201	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	9
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
212.143.158.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.201.73	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
46.244.64.25	Palestinian Territory, Occupied	147.237.77.176	matpash.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	3
46.19.86.205	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	3
46.19.86.243	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
100.92.168.234		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.31	Israel	147.237.76.42	refuah.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
46.244.64.25	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.158.183	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.226	United States	147.237.0.200	m4u.idf.il	drop		drop	1
46.19.86.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.226.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
192.115.248.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.84	United States	147.237.0.33	idf.il	drop		drop	1
176.13.228.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.130.115	Israel	147.237.72.166	aka.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
176.13.10.175	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.84	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.237.88	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.156.147	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.158.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.11.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
80.246.130.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.112	United States	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.200.197	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.13.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
80.246.130.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-04-2016-09:04:07 to 09-04-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	508
2.53.1.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
109.253.157.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
37.26.147.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
2.53.133.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.53.140.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.55.186.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.53.62.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.150.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	4
213.57.247.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.186.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.53.186.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
87.69.36.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.6.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
77.126.0.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.241.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.245.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.25.122	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
96.246.166.69	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/giyus/	Block	2
2.53.172.87	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.211.240	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.139.5.142	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
89.138.115.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
80.246.136.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
194.90.25.122	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.84	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
95.86.119.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
2.53.42.3	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.0.110	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
147.234.241.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
81.218.151.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
109.226.27.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aps	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
176.13.232.117	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.46.42.235	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
2.53.23.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

09-04-2016-09:04:07 to 09-04-2016-10:04:07