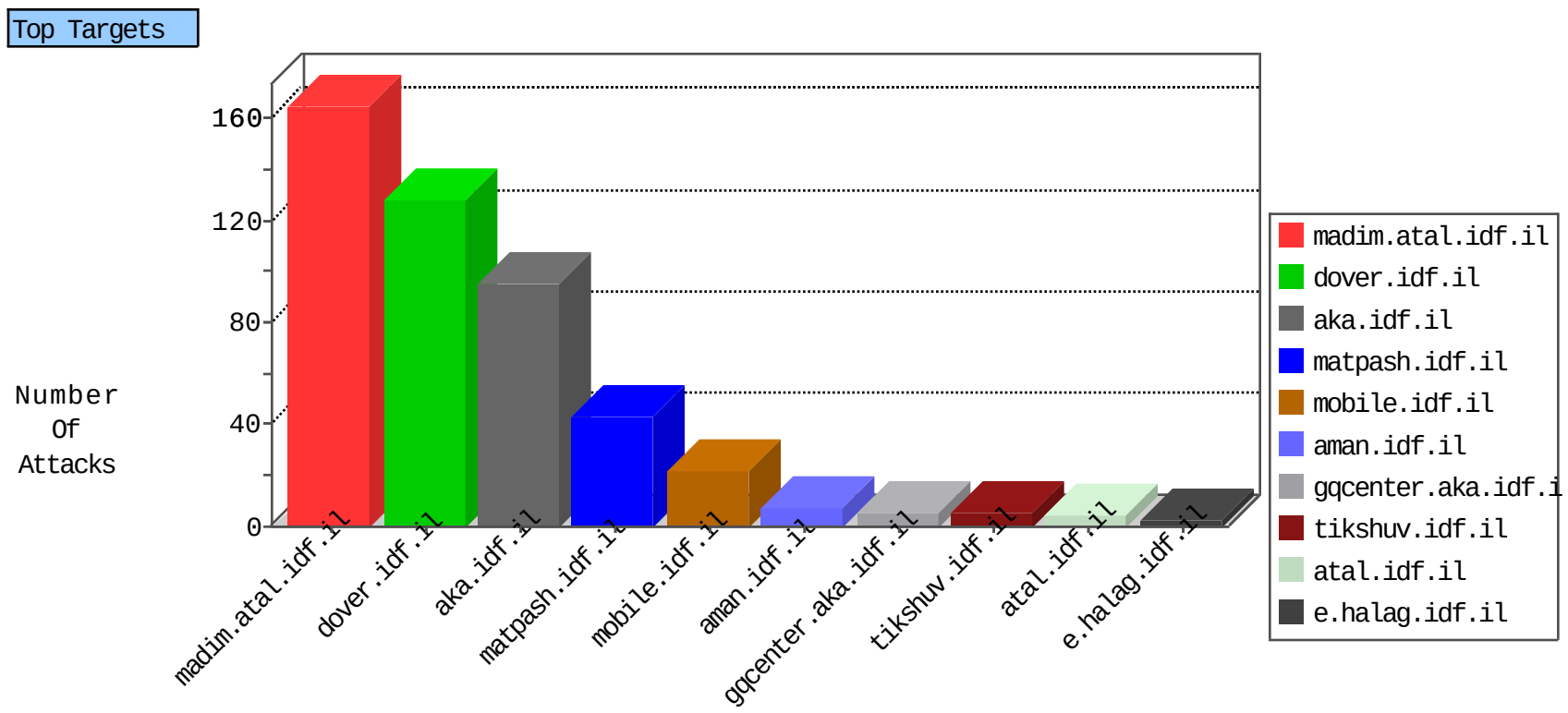
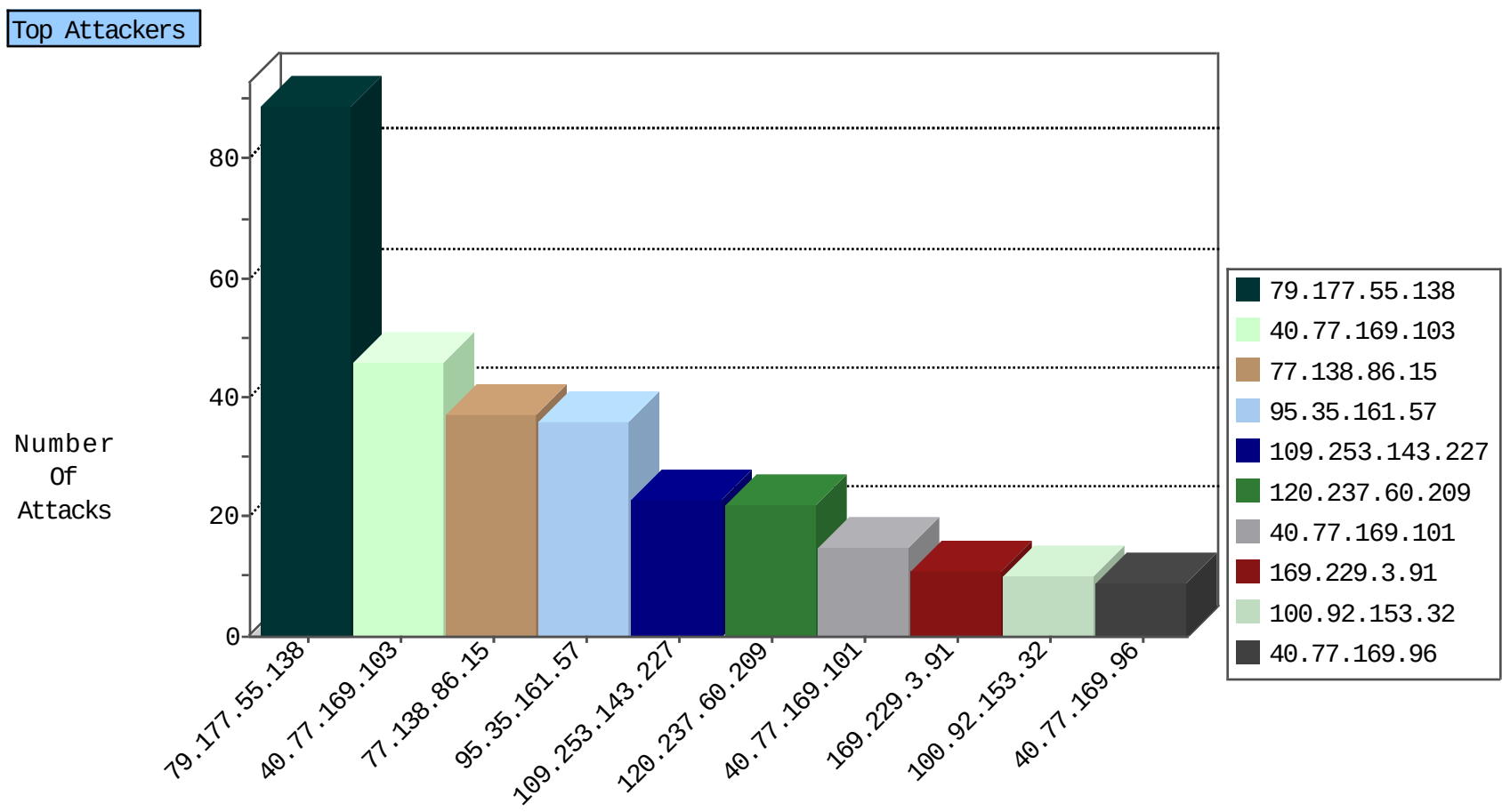
08-25-2016-14:04:02 to 08-25-2016-15:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-25-2016-14:04:02 to 08-25-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.5.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
2.53.31.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
185.24.204.86	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
162.218.211.137	United States	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
103.200.29.42	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
104.148.55.162	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-25-2016-14:04:02 to 08-25-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
151.80.31.159	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-25-2016-14:04:02 to 08-25-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.132.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.122.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.47.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.61.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.214.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.165.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.77.61	Chile	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.83.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.70.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.143.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.136.160.207	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
5.28.134.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
2.53.183.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.99.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.18.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.27.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.29.220.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.84.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.242.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.65.252	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
133.242.3.168	147.237.76.148	Japan	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
132.71.144.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.25.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.136.160.207	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
37.142.40.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-14:04:02 to 08-25-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.138.86.15	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	19
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
100.92.153.32		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.103	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.245.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.108.137.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.129.123	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.31.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
109.253.141.157	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
197.149.176.33	Tanzania, United Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
184.105.247.250	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
109.253.219.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
209.88.157.240	Israel	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
185.24.204.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
133.242.3.168	Japan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.143.80.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.227.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
185.27.106.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1
150.70.173.5	Japan	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
109.253.140.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: Potential network configuration problem detected	Non-compliant TCP packets coming from multiple internal sources were detected. This may result from potential network configuration problem.	drop	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
150.70.173.56	Japan	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.200	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-25-2016-14:04:02 to 08-25-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.55.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
95.35.161.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
109.253.143.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
120.237.60.209	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.237.60.209	Block	15
5.29.175.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
120.237.60.209	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
79.176.133.22	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
2.53.175.227	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.175.227	Block	4
212.150.236.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.241.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
40.77.169.96	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	2
31.168.195.81	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
109.253.143.227	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	2
82.145.209.20	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.112.144	Block	2
157.55.39.109	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
95.86.110.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.19.120.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
82.80.19.242	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
204.79.180.125	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
79.176.73.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
84.108.70.15	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
80.246.136.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.55.142.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
162.216.46.62	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	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
109.253.133.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.132.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl103 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.102.9.85	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
85.64.85.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.19.85.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.140.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
68.180.228.154	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
46.120.100.39	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
82.145.209.20	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.145.209.20	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
120.237.60.209	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1

08-25-2016-14:04:02 to 08-25-2016-15:04:02