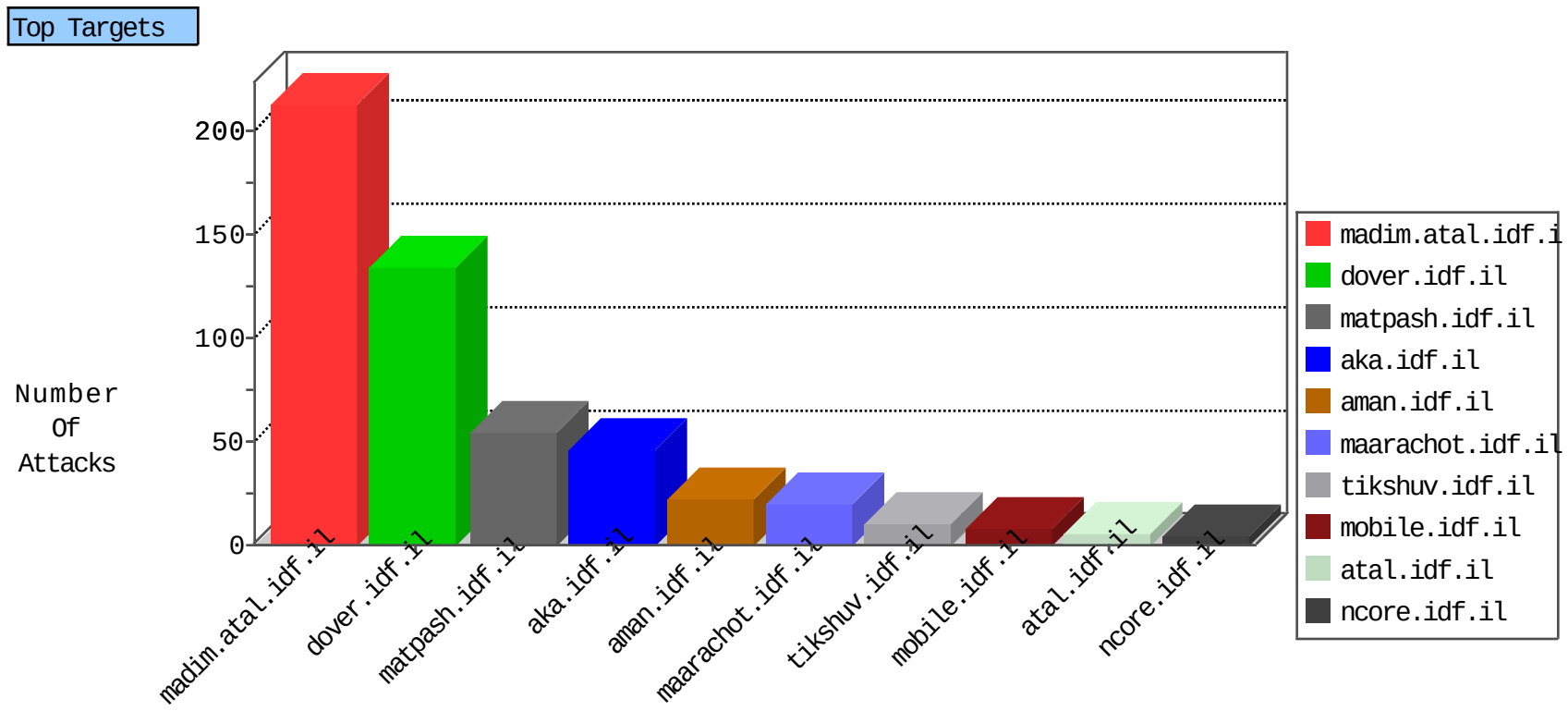
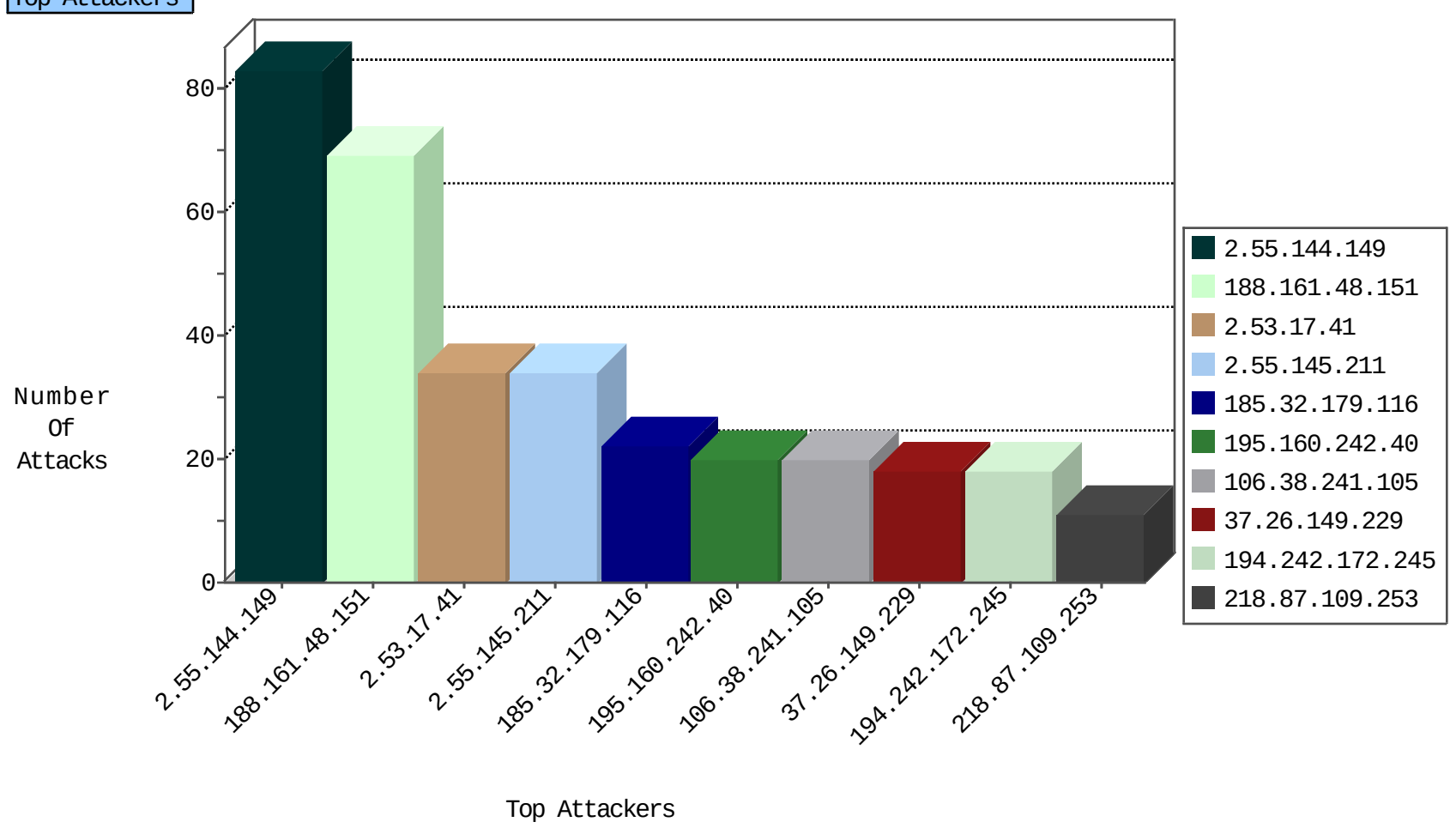
08-21-2016-16:04:03 to 08-21-2016-17:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-21-2016-16:04:03 to 08-21-2016-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
137.74.184.202	Hong Kong	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1

08-21-2016-16:04:03 to 08-21-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	20
51.255.65.49	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
163.172.29.81	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
164.132.161.48	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-16:04:03 to 08-21-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.52.152	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	10
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
91.224.161.69	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.176	Germany	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.117.140.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.161.69	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.8.45	Colombia	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
37.143.82.50	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.161.69	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
37.46.38.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.181.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.87.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.103.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
109.253.201.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.10.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
95.215.60.214	147.237.0.33	Spain	idf.il	ET SCAN Potential SSH Scan	1
66.249.76.79	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
52.27.84.56	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	1
91.224.161.69	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.8.45	Colombia	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.161.69	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
201.232.25.160	147.237.8.45	Colombia	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
91.224.161.69	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.168.225.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.223.90.236	147.237.76.177	Bolivia	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.138.108.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
2.53.136.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.206.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.85.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
79.182.130.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
93.173.167.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.145.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

08-21-2016-16:04:03 to 08-21-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.161.48.151	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	49
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
188.161.48.151	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
62.0.67.44	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.196	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
62.0.211.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.81.199	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
66.102.9.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
181.80.1.251	Argentina	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
85.130.223.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.154.41.17	Israel	147.237.77.216	dover.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
85.130.249.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.114.201.181	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.203.84.84	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
187.40.155.134	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.208.239	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
187.161.165.31	Mexico	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
85.130.249.166	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
176.13.21.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.218.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
49.231.255.45	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
66.102.9.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.248.166	Israel	147.237.72.156	aman.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
109.253.200.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
189.219.117.239	Mexico	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
109.253.200.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1

08-21-2016-16:04:03 to 08-21-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.144.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.53.17.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.55.145.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
185.32.179.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.149.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
194.242.172.245	France	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	14
2.53.167.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.130.2	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
77.138.2.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	3
109.253.202.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.242.172.245	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
23.27.45.60	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	2
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.188	Block	2
2.53.49.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.160.38	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
156.208.78.42	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.182.59.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/common/	Block	2
84.108.232.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/5/71575.pdfא	Block	2
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	2
37.26.147.170	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
85.64.56.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
77.139.168.86	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/klali/default.asp	Block	1
2.55.31.155	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/ kiosk.aspx	Block	1
189.218.238.99	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
46.19.86.7	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.165	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-11428-he/cogat.aspx	Block	1
80.246.136.233	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
189.219.165.81	Mexico	147.237.77.216	dover.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
77.126.51.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
62.90.2.52	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
176.13.246.184	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
87.70.30.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.139.208.178	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
189.219.18.28	Mexico	147.237.0.15	kosher-kravi.idf.il	Redundant HTTP Headers from 189.219.18.28	Block	1
66.249.76.30	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
109.253.202.141	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
31.13.100.118	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/71575.pdfא	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
82.80.48.26	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/admin	Block	1
189.219.165.81	Mexico	147.237.77.226	www.chamatz.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.22.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
45.245.8.188	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
201.172.52.254	Mexico	147.237.76.200	eitan.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.219.82.64	Mexico	147.237.72.156	aman.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/62939.pdf	Block	1
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1

08-21-2016-16:04:03 to 08-21-2016-17:04:03