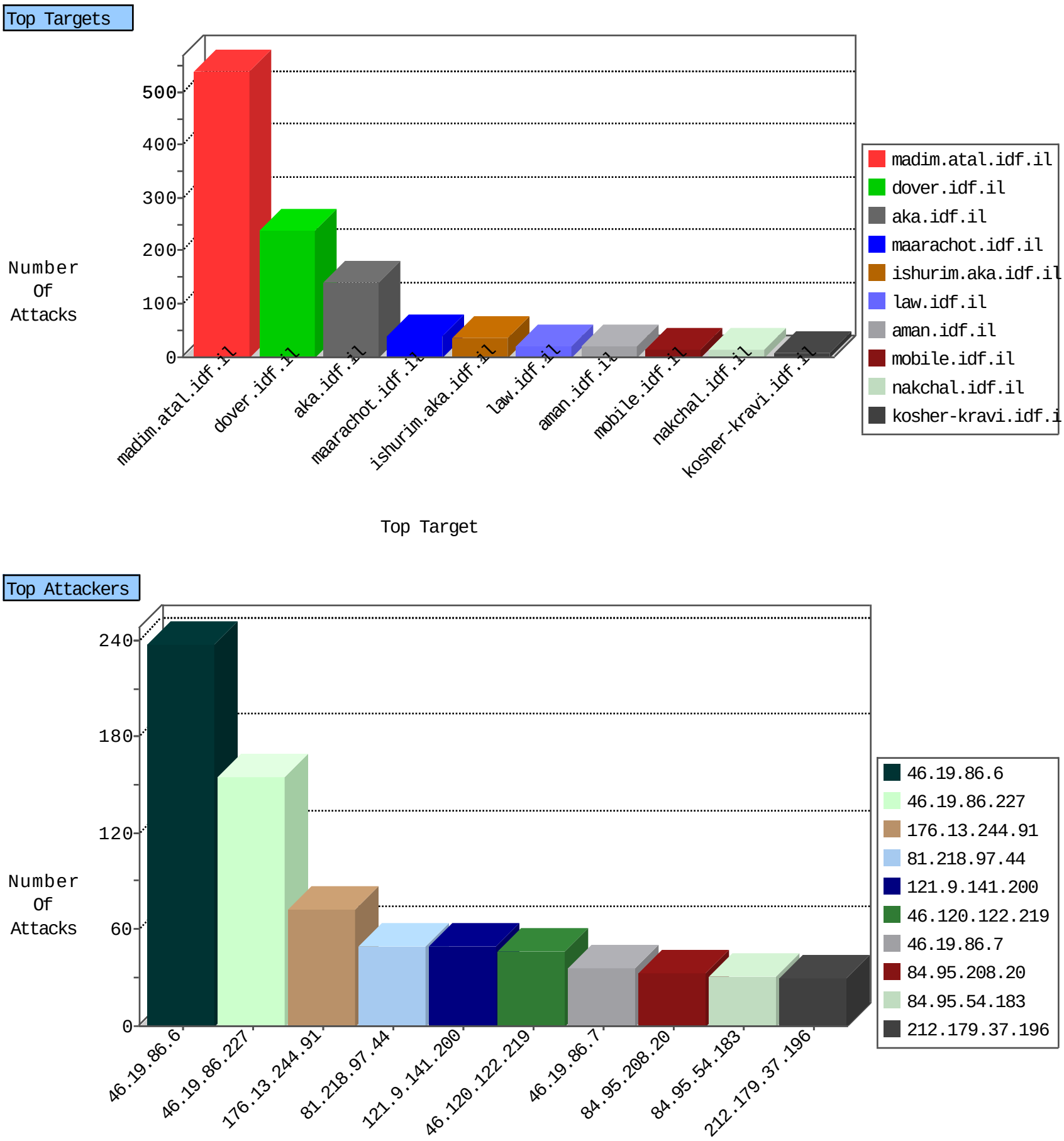
08-30-2016-10:04:05 to 08-30-2016-11:04:05

IDF Under Attack
Daily Report



08-30-2016-10:04:05 to 08-30-2016-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
91.210.104.40	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
79.182.21.51	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
91.210.104.40	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-30-2016-10:04:05 to 08-30-2016-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.170.125	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.107	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-30-2016-10:04:05 to 08-30-2016-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	18
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	7
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	6
79.182.130.75	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
80.246.130.186	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
79.177.122.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
85.113.107.165	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
185.110.132.201	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
84.109.1.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.153.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
176.13.236.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
200.195.135.82	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
147.236.238.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.195.135.82	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -f -sS	1
77.127.74.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.80.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.188.150	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.169.70.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.53.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.121.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.118.166.18	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
46.121.13.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.136.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	1
185.110.132.201	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
87.68.14.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.72.217	Ukraine	e.idf.il	ET SCAN Potential SSH Scan	1
85.65.104.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
80.246.139.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.106.44.149	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.49.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.195.135.82	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
77.139.102.56	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.230.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.188.150	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.28.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.70.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-30-2016-10:04:05 to 08-30-2016-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.54.183	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	31
212.179.37.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
81.218.97.44	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.137.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
81.218.97.44	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
81.218.97.44	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	13
84.111.246.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.81	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	10
62.207.60.228	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
62.0.211.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.207.60.231	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
84.111.246.13	Israel	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	6
109.253.159.63	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
89.138.206.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.236.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
92.24.47.104	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
66.249.93.103	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	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	3
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.227.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
59.88.35.219	India	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
80.246.130.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.67.100.78	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
176.13.228.197	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
87.71.19.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.106.47.228	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.69.133.245	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.113.82.72	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.108.207.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.69.133.247	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.191.201.45	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.219.120.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
192.115.248.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.166.130.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.241.83	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.8.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
74.82.47.59	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-30-2016-10:04:05 to 08-30-2016-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155
176.13.244.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
121.9.141.200	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.141.200	Block	35
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	12
37.26.148.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
89.237.116.235	France	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	7
121.9.141.200	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
121.9.141.200	China	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
176.13.243.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
77.138.84.43	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/matash/login	Block	5
109.64.193.138	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	5
83.110.79.5	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
89.237.116.235	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
83.110.103.103	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.185.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
5.29.71.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.40.239	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
109.64.193.138	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 109.64.193.138	Block	3
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
77.138.84.43	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
2.53.130.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.237.116.235	France	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 89.237.116.235	Block	2
217.132.124.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
121.9.141.200	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
37.142.180.93	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.18.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
81.218.251.251	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.57.145.118	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/piwik.php	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
80.178.208.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.193.138	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.73.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/09022011yezu.aspx	Block	1

08-30-2016-10:04:05 to 08-30-2016-11:04:05