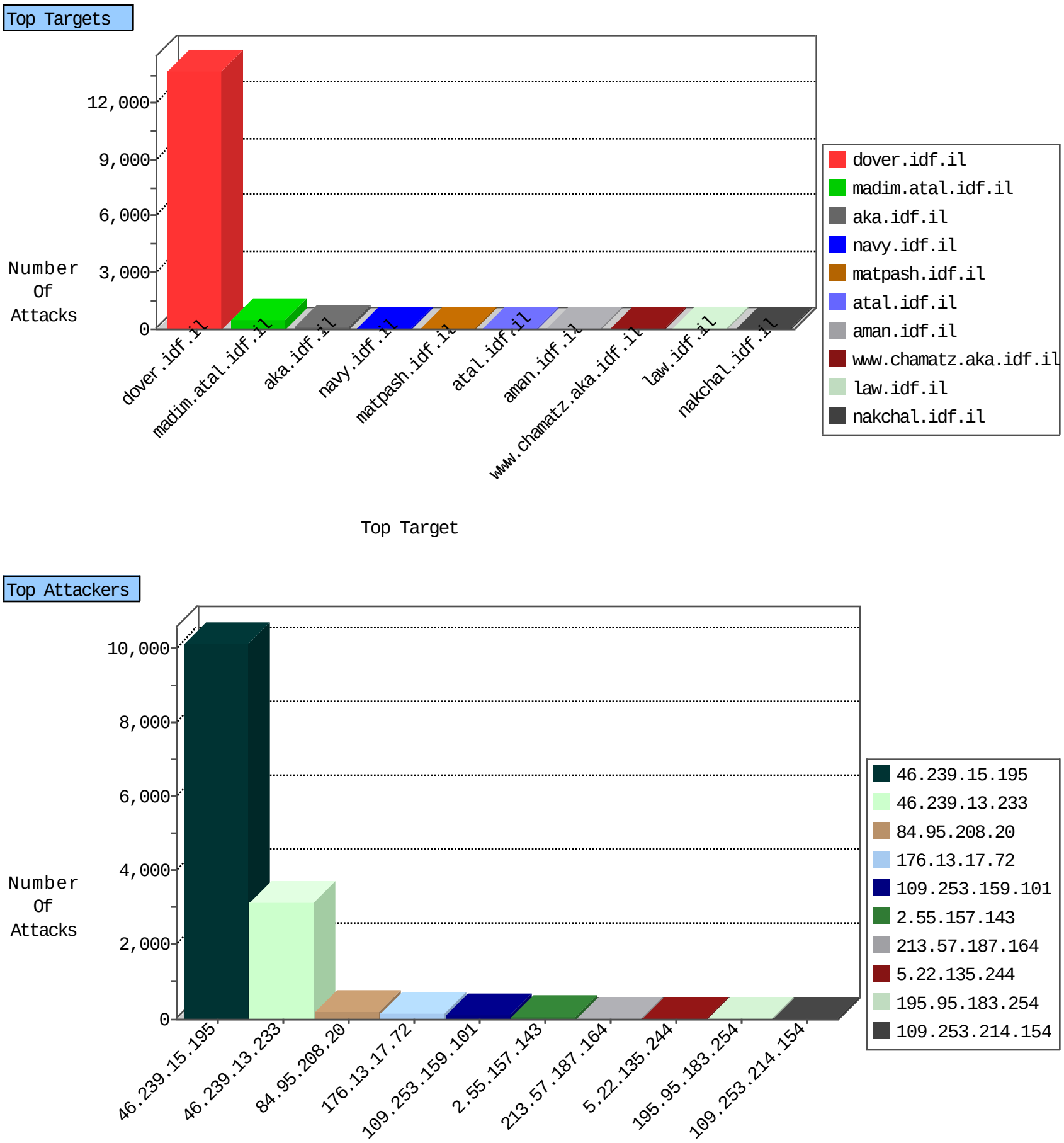
08-28-2016-11:04:00 to 08-28-2016-12:04:00

IDF Under Attack Daily Report



08-28-2016-11:04:00 to 08-28-2016-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.214	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
207.232.54.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.65.195.141	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.248.167.131	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
80.82.78.27	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
80.82.78.27	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
80.82.78.27	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-28-2016-11:04:00 to 08-28-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-28-2016-11:04:00 to 08-28-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.178.171.58	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	26
180.151.140.122	147.237.77.121	India	e.navy.idf.il	ET SCAN Potential SSH Scan	2
46.227.67.172	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
31.154.234.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.31	Ukraine	nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.22.134.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.181.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.164.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
79.179.142.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.76.34	India	yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.176.59.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.8.46	India	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.11	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
178.220.165.231	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 4096	1
217.132.38.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.210.148.91	147.237.76.147	France	chinuch.aka.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
109.67.127.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.116.81	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
103.207.37.92	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.77.234	India	halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.244.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.77.216	India	dover.idf.il	ET SCAN Potential SSH Scan	1
84.108.127.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.131.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.76.200	India	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.182.44.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
180.151.140.122	147.237.72.14	India	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
68.180.228.29	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
180.151.140.122	147.237.0.16	India	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.219.162.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.220.165.231	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 3072	1
213.233.85.46	147.237.72.166	Romania	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.88.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.98.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-28-2016-11:04:00 to 08-28-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10044
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2955
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	100
5.22.135.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
195.95.183.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
178.195.102.104	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.13.16.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.232.54.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
81.138.8.36	United Kingdom	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
46.19.86.29	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
46.19.85.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.66.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.92.227.96		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.43.68.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.29.244.55	Israel	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
46.43.100.207	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.121.138.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.20.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.156.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.204.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
2.50.0.75	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.176.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.131.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.125	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.11.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.173.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.198.151.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.20.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.154.81.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.102.169.113	Israel	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
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.94.54.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

08-28-2016-11:04:00 to 08-28-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
109.253.159.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	100
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	58
2.55.157.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
213.57.187.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
109.253.214.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.13.224.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
176.13.1.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	5
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	4
2.53.136.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.139.125.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	3
176.13.0.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
37.26.149.186	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation	Block	2
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.178.8.213	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
176.13.3.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.11.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
79.183.20.124	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.60.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.238.166.111	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin	Block	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
188.120.148.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
66.249.83.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.69.145	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
192.115.200.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
79.183.99.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
213.57.156.114	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.94.54.154	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
5.29.248.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
88.202.218.237	United Kingdom	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	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
46.121.69.145	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
37.238.166.111	Iraq	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	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
2.55.186.159	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.175	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
77.139.242.92	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotfaq.aspx	Block	1

08-28-2016-11:04:00 to 08-28-2016-12:04:00