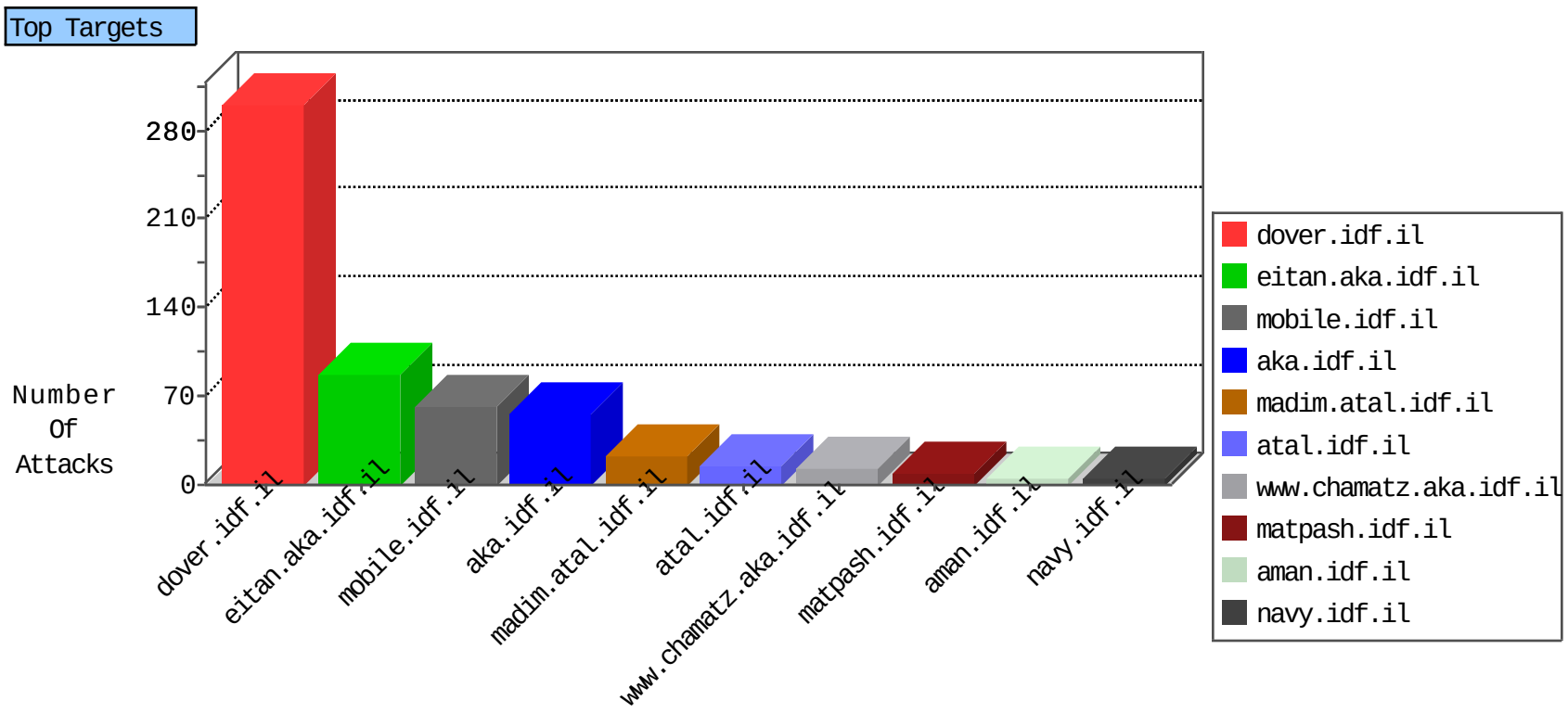
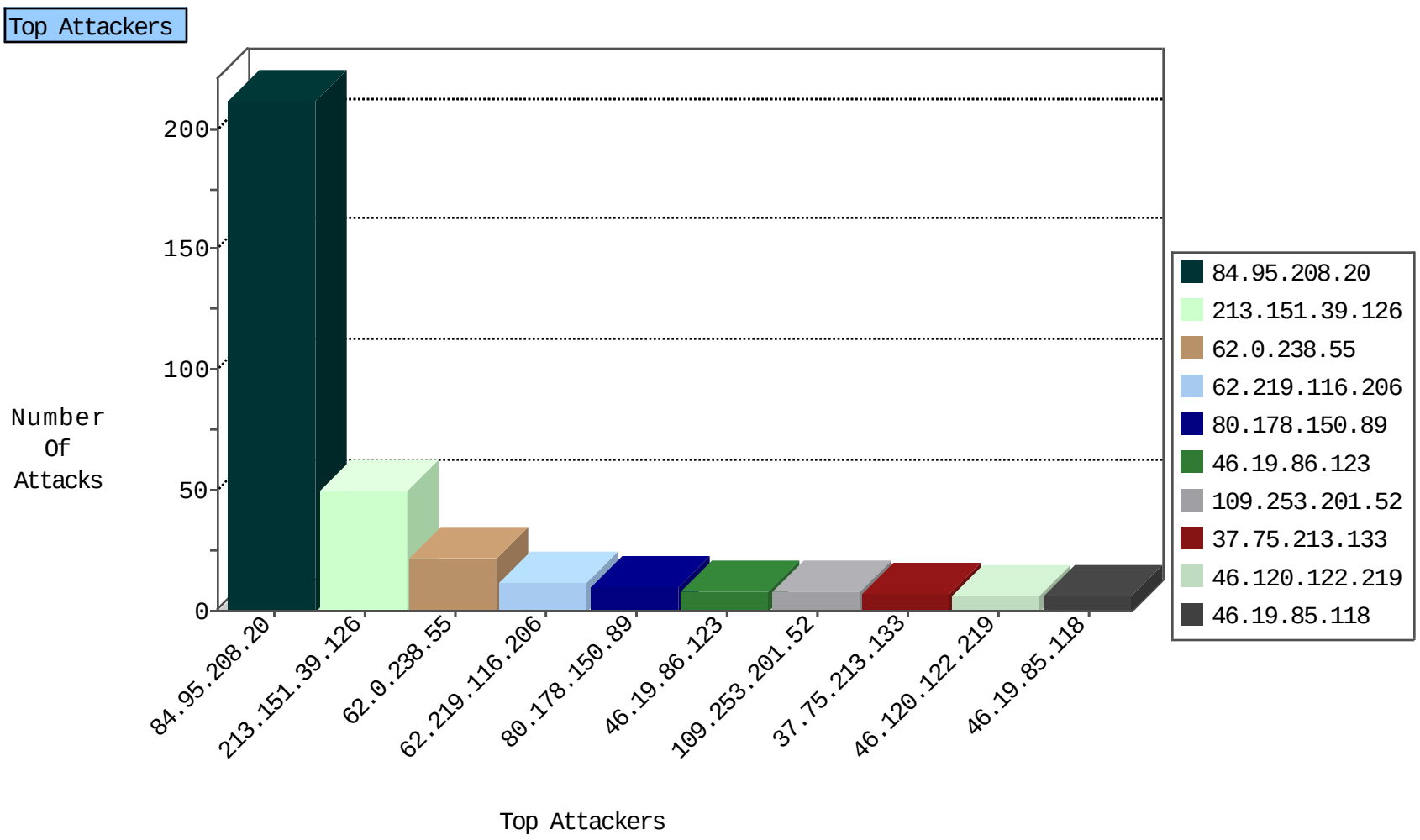
08-31-2016-12:04:07 to 08-31-2016-13:04:07

IDF Under Attack
Daily Report





08-31-2016-12:04:07 to 08-31-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.116.102.64	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
120.132.50.135	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
219.87.191.219	Taiwan	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
153.228.137.116	Japan	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
179.99.200.39	Brazil	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
91.230.107.174	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
94.102.49.190	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1

08-31-2016-12:04:07 to 08-31-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-31-2016-12:04:07 to 08-31-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	6
79.181.104.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
87.115.230.45	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
212.179.155.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
80.178.92.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.77.234	Chile	halag.idf.il	ET SCAN NMAP -sS window 1024	1
5.15.192.61	147.237.8.28	Romania	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
193.201.225.149	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.3.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.77.90.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.244.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.56.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.197.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
38.111.147.88	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
87.236.194.161	147.237.77.74	Czech Republic	law.idf.il	ET SCAN NMAP -sS window 1024	1
23.101.61.176	147.237.72.166	Ireland	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.243.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.44.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.139.34.20	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
84.95.208.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.117.136.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.15.192.61	147.237.8.28	Romania	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
79.183.76.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
79.181.23.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.24.204.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.18.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.25.42.125	147.237.77.216	Japan	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.180.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.139.34.20	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
84.95.208.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-31-2016-12:04:07 to 08-31-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.151.39.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.219.116.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.238.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.150.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.118.36.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.144.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.75.213.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.243.58.63	Russian Federation	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
84.94.73.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.197.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.78.56.72	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.75.213.133	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
176.13.22.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.228.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.217.84	Israel	147.237.77.243	mobile.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
176.13.237.201	Israel	147.237.72.166	aka.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
176.13.21.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.151.36.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.132.138.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.86.112.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
222.35.18.100	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.134.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
146.185.56.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
83.220.46.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.150.125.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.138.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.243.192	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
79.177.221.194	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.245.54	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
193.182.147.8	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.232.251	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

08-31-2016-12:04:07 to 08-31-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	102
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	85
109.253.201.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.55.55.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.234.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.211.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
77.139.6.178	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	4
176.13.248.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.156.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.228.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
131.253.27.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.147.237	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
108.171.128.175	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
80.178.150.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.178.150.89	Block	3
89.138.105.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.250.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.139.120.18	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
37.26.146.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.178.215.173	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
82.109.66.147	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.137.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.235.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.148.38	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.0.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.217.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.139.65.94	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
2.53.178.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
82.109.66.145	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.239	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
157.55.39.194	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.190.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22261-he/dover.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
82.109.66.150	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.93.187	Israel	147.237.76.86	navy.idf.il	Multiple URL is Above Root Directory from 66.249.93.187	Block	1
2.53.48.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
108.171.128.175	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 108.171.128.175	Block	1
183.79.94.43	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1

08-31-2016-12:04:07 to 08-31-2016-13:04:07