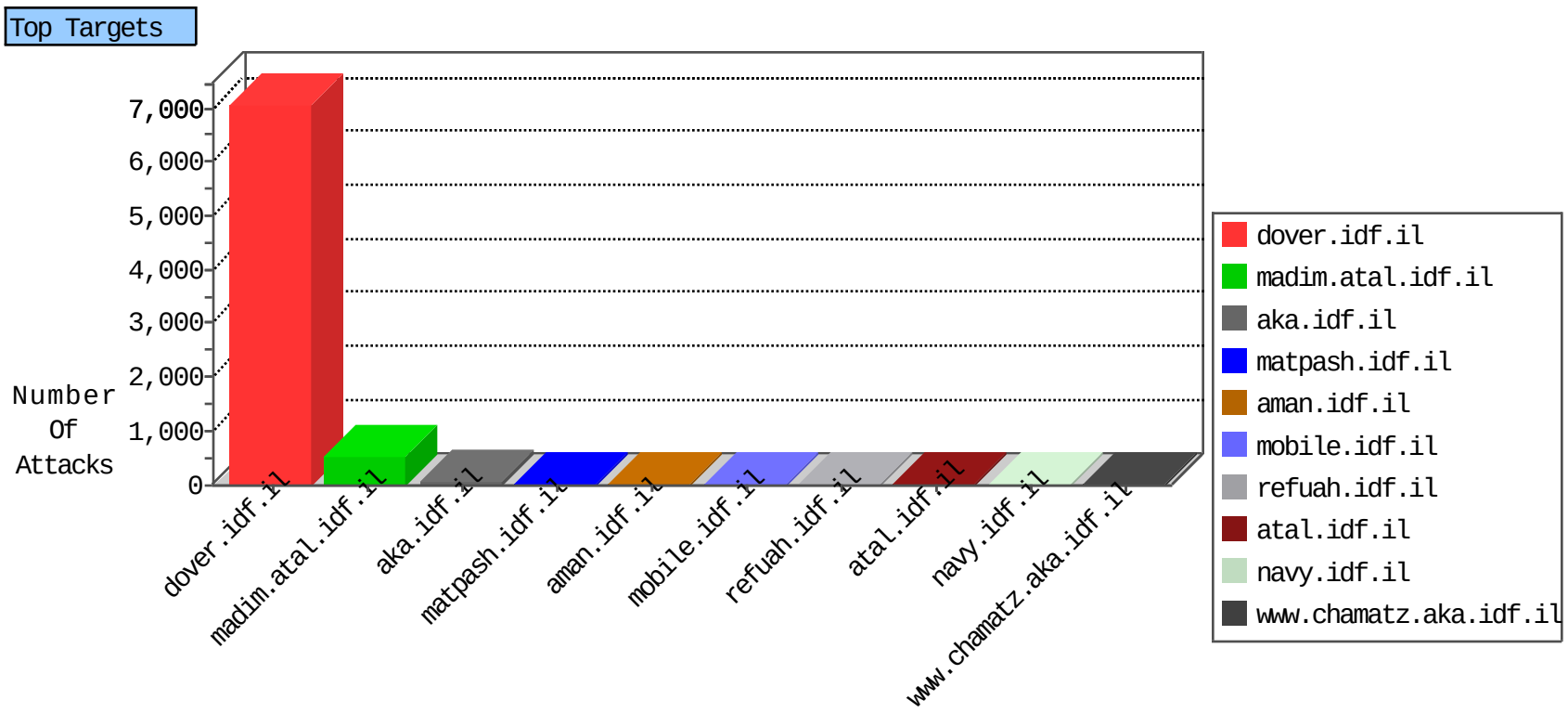
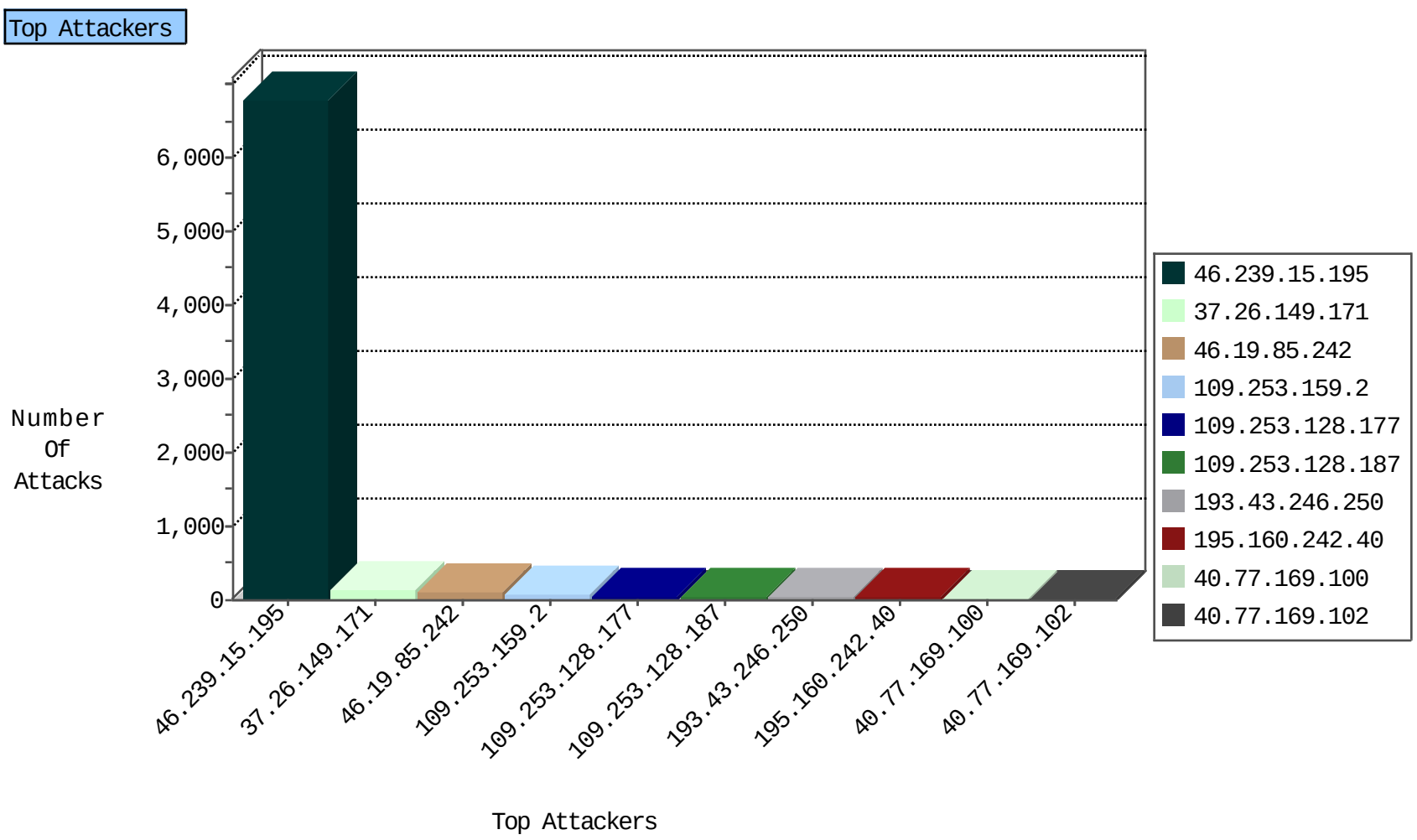
08-28-2016-09:04:03 to 08-28-2016-10:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-09:04:03 to 08-28-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
163.172.227.198	United Kingdom	147.237.76.202	e.halag.idf.il	Black List	drop	1
104.238.184.170	United Kingdom	147.237.76.42	refuah.idf.il	Black List	drop	1
109.65.188.200	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-28-2016-09:04:03 to 08-28-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
198.20.87.98	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-28-2016-09:04:03 to 08-28-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
123.206.73.185	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.129.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.176.80.201	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
77.139.29.232	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.33.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.246.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.67.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.93.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.67.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.179.184.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.56.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.206.73.185	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.23.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.254.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.40.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
89.138.151.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
84.229.72.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.132.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.127.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.208.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.189.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.178.184.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-28-2016-09:04:03 to 08-28-2016-10:04:03

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	6645
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
82.213.48.225	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
176.13.234.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
109.253.156.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.103	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
59.56.69.195	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.181.206.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
212.14.243.126	Palestinian Territory, Occupied	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
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
46.19.86.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.218.57.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.195	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
192.198.151.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.201.167	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
134.191.232.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.230.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.210.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
138.246.253.19	Germany	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.253.137.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.211.167	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
167.220.232.104	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
109.253.145.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.239.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.232	United States	147.237.0.200	m4u.idf.il	drop		drop	1
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
176.13.9.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
202.28.10.20	Thailand	147.237.77.74	law.idf.il	drop	SAM rule	drop	1

08-28-2016-09:04:03 to 08-28-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
109.253.159.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
109.253.128.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
109.253.128.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.53.146.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.23.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.228.185.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.228.185.73	Block	5
37.26.147.209	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.147.209	Block	4
80.246.136.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.138.245.28	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	3
176.13.22.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.56.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.103.160.130	Greece	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.159.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.185.73	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/0/	Block	3
93.173.227.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.4.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.235.121	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/kiosk.aspx	Block	2
180.191.61.7	Philippines	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.139.5.195	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	2
180.191.61.9	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.184.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
2.53.11.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
37.26.147.204	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
180.191.61.4	Philippines	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 180.191.61.4	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
84.94.235.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/http:/main/giyus/default/script	Block	1
2.53.159.123	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
176.13.224.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
85.64.104.160	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.64.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/394.pdftextgreater	Block	1
192.116.188.73	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
180.191.61.4	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.177.140.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-28-2016-09:04:03 to 08-28-2016-10:04:03