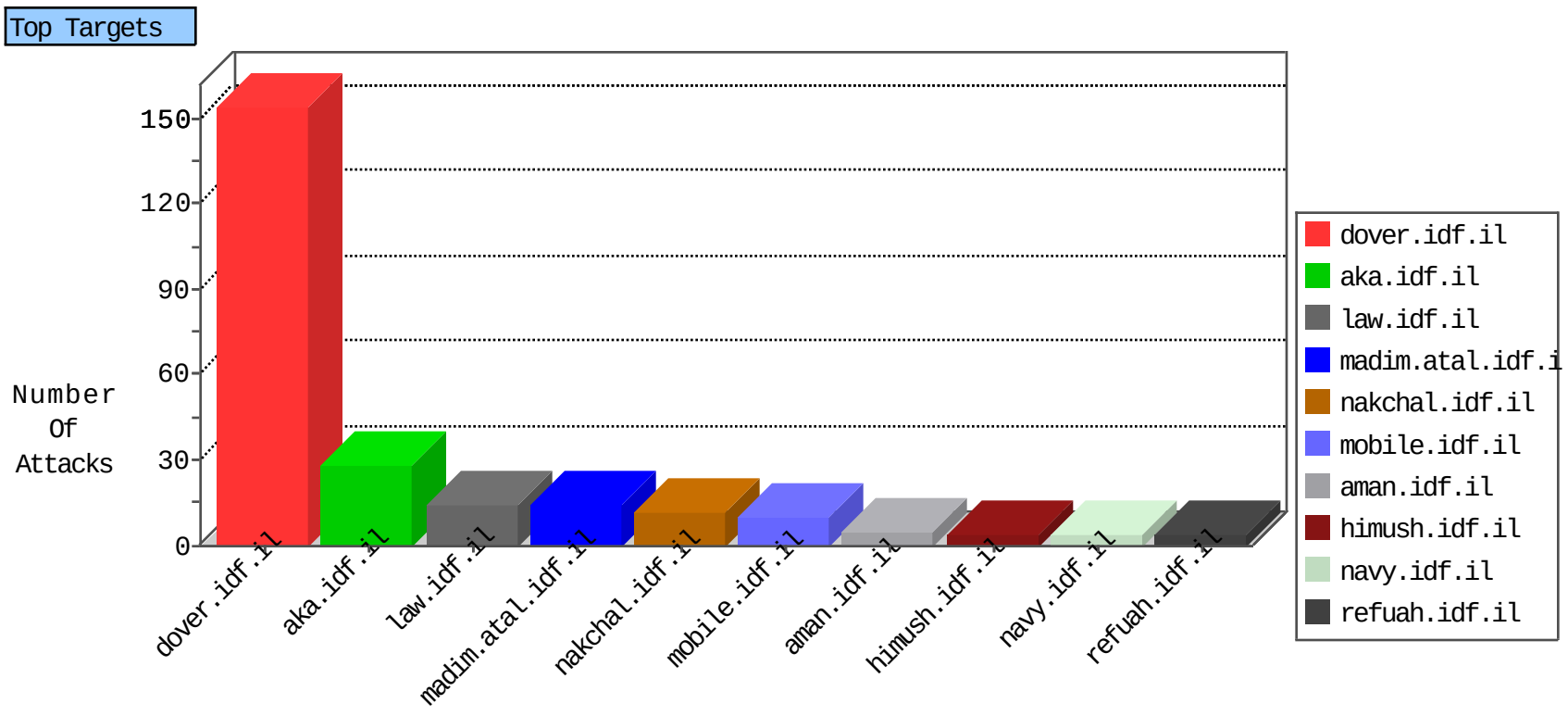
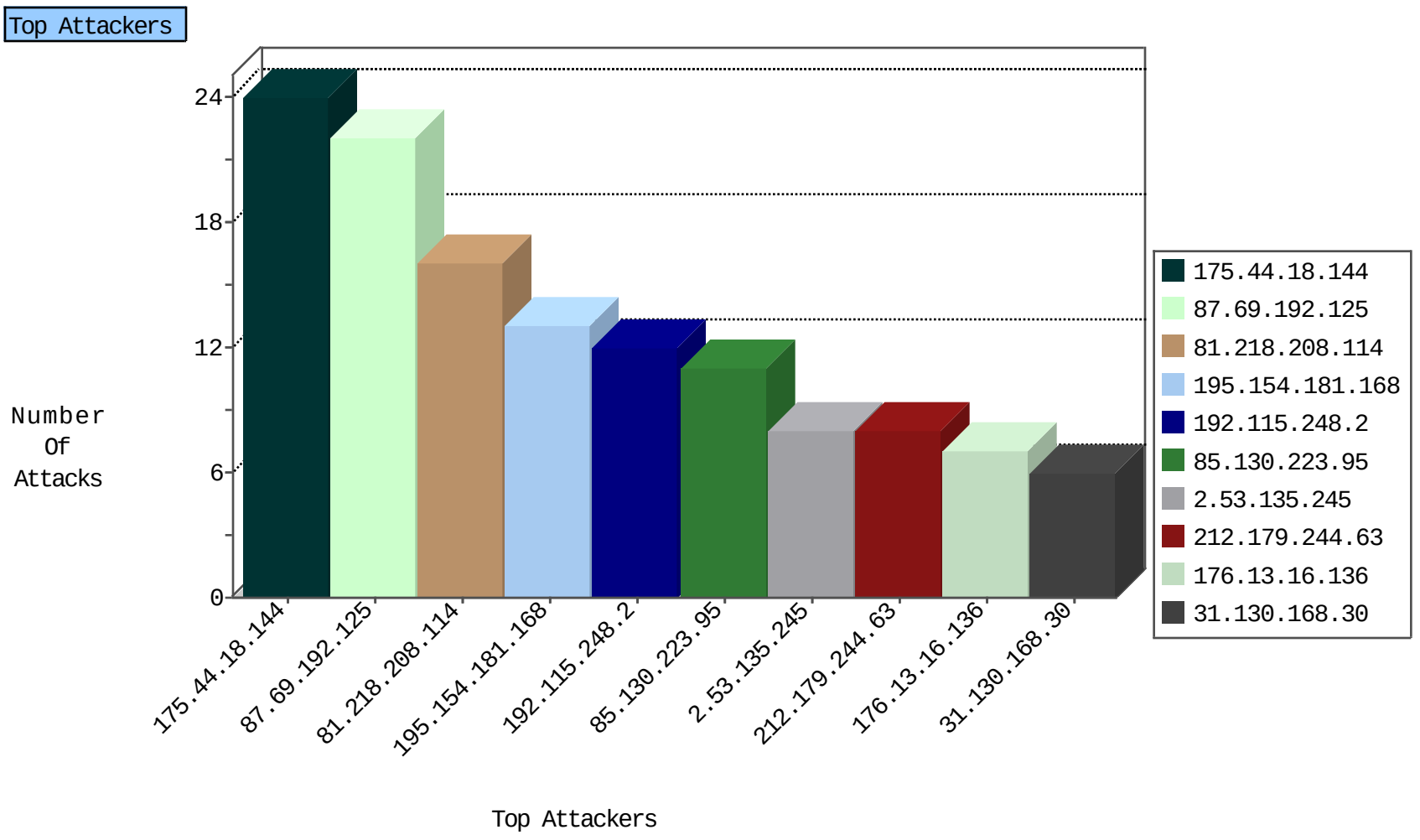
08-17-2016-14:04:08 to 08-17-2016-15:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-17-2016-14:04:08 to 08-17-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.0.0.1		147.237.72.156	aman.idf.il	Black List	drop	1
82.221.105.6	Iceland	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.146.185	United States	147.237.76.30	himush.idf.il	Black List	drop	1
93.158.200.118	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
79.183.47.13	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
93.158.200.118	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-17-2016-14:04:08 to 08-17-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.99.130	Netherlands	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
164.132.161.16	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.38	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-17-2016-14:04:08 to 08-17-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.29.11.182	147.237.8.27	Latvia	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
84.108.99.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.149.74	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
132.74.210.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.132.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.135.131.60	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
62.90.235.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.239.248.72	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
41.34.20.222	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
109.226.14.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
213.57.134.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.26.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.167.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.152.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.21.228.166	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.144.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.149.74	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
132.66.223.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.33.212	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
115.239.248.72	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.108.10.31	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.33.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.232.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.168.29	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
213.8.204.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.216.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-17-2016-14:04:08 to 08-17-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.192.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
85.130.223.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.135.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.16.136	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	7
52.28.40.166	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.130.168.30	Czech Republic	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
193.175.245.253	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.73.34.77	Germany	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
85.130.223.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.241.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.67	United States	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
109.253.130.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.13.102.107	Ireland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
176.13.0.88	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
66.249.64.128	Israel	147.237.0.33	idf.il	drop		drop	1
109.253.193.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.201.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.142.253.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-17-2016-14:04:08 to 08-17-2016-15:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
175.44.18.144	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.18.144	Block	17
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
212.179.244.63	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
175.44.18.144	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
80.246.130.175	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
37.142.182.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
131.253.27.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.18.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	3
131.253.25.190	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
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
213.178.237.82	Syrian Arab Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
37.26.148.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	2
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
82.81.137.130	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
195.154.181.168	France	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
195.154.181.168	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/license.php	Block	1
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 81.218.208.114	Block	1
79.181.176.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
173.252.90.87	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20575-he/idfgdover.aspx	Block	1
109.65.187.211	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 81.218.208.114	Block	1
31.13.97.122	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/size220x0/1738.jpg	Block	1
195.154.181.168	France	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
132.66.223.243	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
195.154.181.168	France	147.237.77.243	mobile.idf.il	Distributed PHP Attempt	Block	1
85.64.246.166	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.133.102.196	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
195.154.181.168	France	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 195.154.181.168	Block	1
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 81.218.208.114	Block	1
79.183.48.88	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.252.90.101	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/1/size220x0/1751.jpg	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
109.67.191.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
81.218.208.114	Israel	147.237.77.216	dover.idf.il	NULL Character in Method ¥T¾'*ý_¶íñ[[#12]]?	Block	1
195.154.181.168	France	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
81.218.208.114	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL ıIk˙:,e¶[[#17]]¥¯f9¸an¾ŋŽ¿w[[#19]]˙¸-ˆƒl¹o˙[[#28]][[#26]]>ŦŒ¼•€—ž¶	Block	1
132.66.223.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1154-he/	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
62.128.41.130	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/homas/site/default.aspx	Block	1
195.154.181.168	France	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/license.php	Block	1
87.68.30.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
195.154.181.168	France	147.237.72.156	aman.idf.il	PHP Attempt	Block	1

08-17-2016-14:04:08 to 08-17-2016-15:04:08