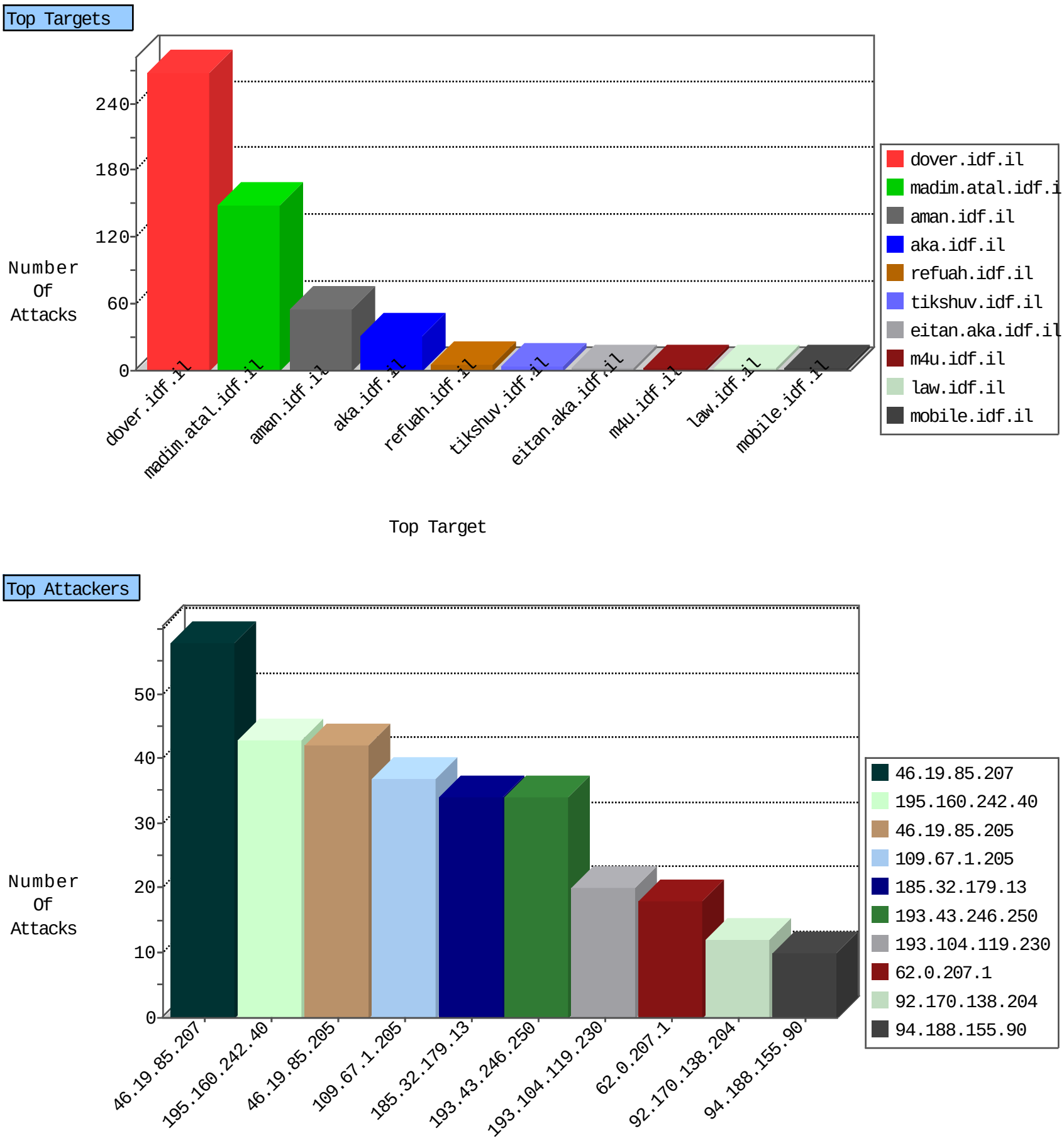
08-22-2016-09:04:07 to 08-22-2016-10:04:07

IDF Under Attack
Daily Report



08-22-2016-09:04:07 to 08-22-2016-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.1.205	Israel	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	797
109.67.1.205	Israel	147.237.72.156	aman.idf.il	JLM_Purple_Con_Limit_Tcp	drop	154
185.97.132.82	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	60
193.104.119.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
109.67.131.144	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.116.114.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.64.118.67	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.115.177.203	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.66.63.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
162.243.195.60	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
194.165.146.148	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
91.230.121.156	Ukraine	147.237.76.34	yohalan.idf.il	Black List	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
137.74.157.88	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
195.154.172.204	France	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
109.65.139.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.i	Black List	drop	1
2.55.6.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-22-2016-09:04:07 to 08-22-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.194.31	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
94.102.49.190	Netherlands	147.237.76.198	e.yohalan.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
51.255.65.72	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.17	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.77	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.79	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-09:04:07 to 08-22-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2

08-22-2016-09:04:07 to 08-22-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
62.0.207.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
193.104.119.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
92.170.138.204	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
94.188.155.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.180.196.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.71.55.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.61.251.229	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.160.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
77.75.78.164	Czech Republic	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
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.139.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.63.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.142.239.139	Israel	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
84.108.102.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.239.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.179.10.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.122.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.166.199.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.228.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.93.246.10	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
14.141.216.206	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.168.249.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
87.69.107.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.161	Israel	147.237.0.33	idf.il	drop		drop	1
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
194.165.146.148	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.15.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.145.176	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
84.109.234.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	drop		drop	1
195.154.172.204	France	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.247.208	United States	147.237.0.200	m4u.idf.il	drop		drop	1
157.55.39.92	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
188.42.240.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-22-2016-09:04:07 to 08-22-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
185.32.179.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.17.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
91.227.164.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
91.227.165.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.162.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.131.44	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.13.192.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
109.253.243.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.25.91.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
2.55.177.80	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.143.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.111.94.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lobby	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
188.120.135.12	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.191.187	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.199.195.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.121.45.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	1
180.76.15.19	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
5.29.62.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
2.53.145.154	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.216.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
194.90.25.122	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/style/shared/reset.css	Block	1
109.253.135.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
213.57.127.42	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.168.170.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.53.168.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.114.108.65	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	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
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.223.65	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
2.55.147.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
220.255.219.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
31.168.170.190	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
2.53.171.162	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.199.69.254	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.150.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.39	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
2.53.129.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

08-22-2016-09:04:07 to 08-22-2016-10:04:07