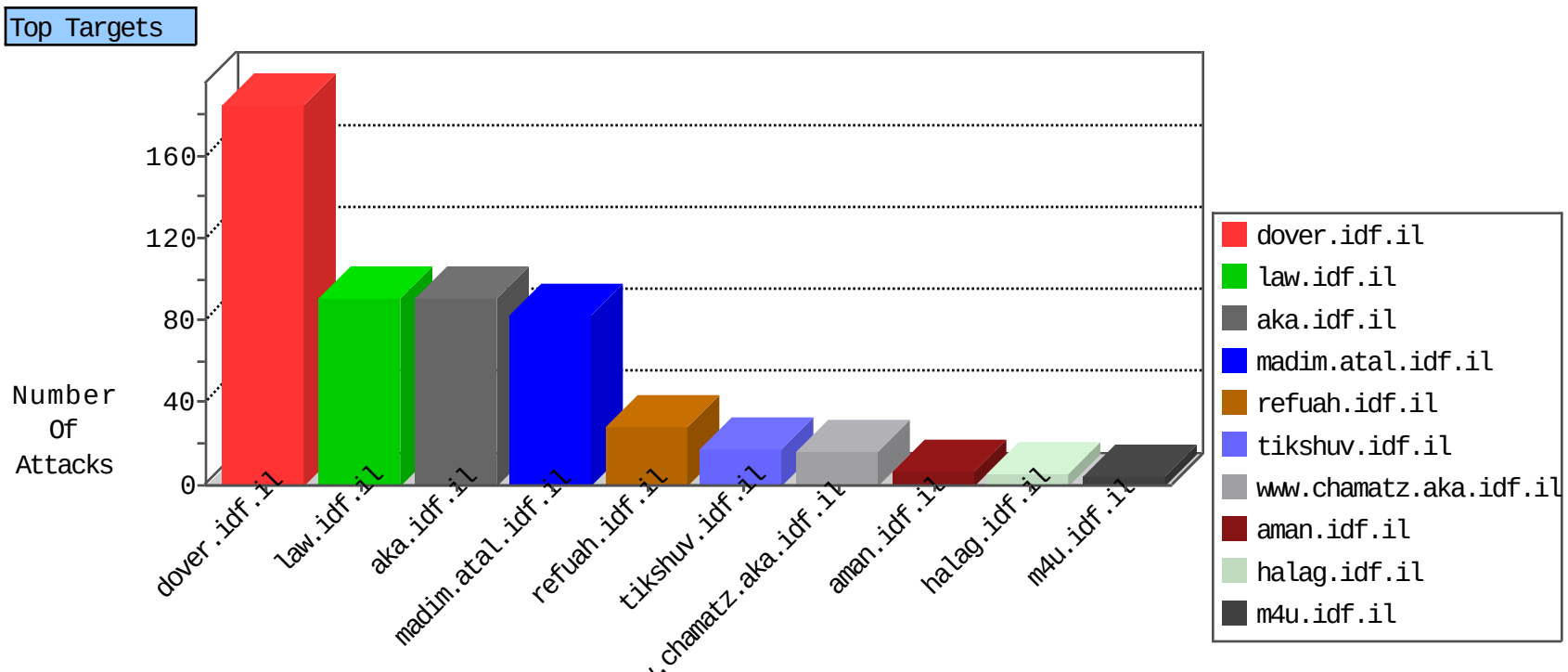
08-18-2016-14:04:03 to 08-18-2016-15:04:03

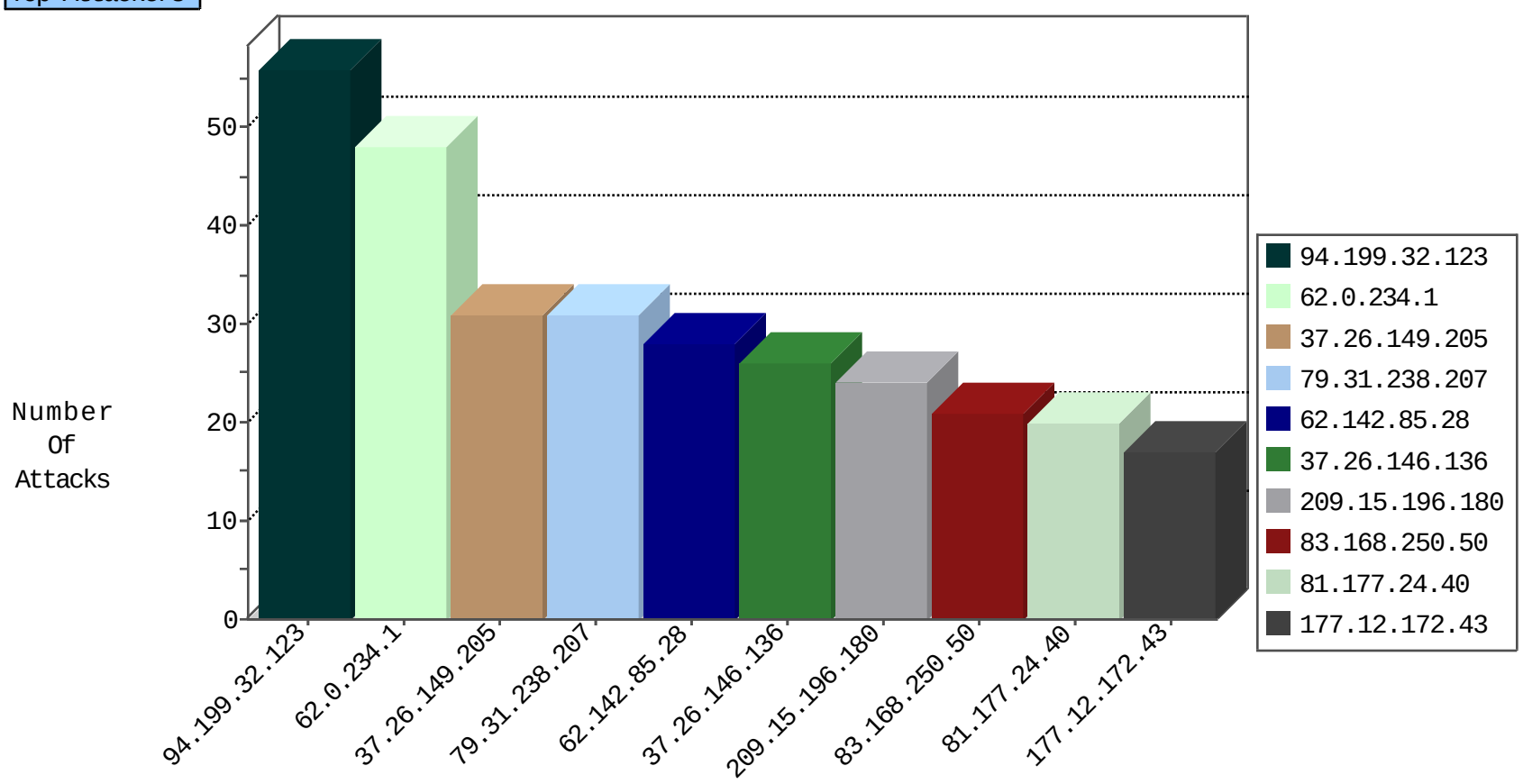
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-18-2016-14:04:03 to 08-18-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.169.18	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
104.148.55.162	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.253.205.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.80.78.2	Israel	147.237.72.166	aka.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
82.80.78.2	Israel	147.237.77.216	dover.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
2.53.2.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

08-18-2016-14:04:03 to 08-18-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.199.32.123	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
177.12.172.43	Brazil	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
94.199.32.123	Turkey	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
209.15.196.180	Canada	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
212.68.146.35	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.180	Canada	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.203.204.143	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.154.12	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.88.198.223	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.177.24.40	Russian Federation	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.180	Canada	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.196.22.55	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.180	Canada	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
216.119.125.57	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
178.6.246.231	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
94.199.32.123	Turkey	147.237.77.74	law.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	3
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.53	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
184.168.27.118	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
195.74.38.14	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-18-2016-14:04:03 to 08-18-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.199.32.123	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	32
81.177.24.40	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	14
113.108.10.31	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.169	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.53.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.178.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-18-2016-14:04:03 to 08-18-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.234.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.31.238.207	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
62.142.85.28	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
83.168.250.50	Sweden	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	13
79.182.23.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
83.168.250.50	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
66.102.9.38	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
62.0.234.1	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
177.185.192.98	Brazil	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
144.76.29.162	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.198.138	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	3
84.94.62.64	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.16.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.117.106.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.165.197.142	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
177.12.172.43	Brazil	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
109.253.135.160	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
176.13.241.153	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
141.212.122.102	United States	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
141.212.122.103	United States	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
109.67.121.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.33	idf.il	drop	SAM rule	drop	1
195.154.172.204	France	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1

08-18-2016-14:04:03 to 08-18-2016-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
37.26.146.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
77.138.99.152	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	7
132.74.28.58	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
79.253.50.219	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	5
109.64.89.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	3
176.13.241.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.7.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.154.7.2	Block	3
80.246.138.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.140.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.9.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.138.220.97	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
66.249.65.138	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 66.249.65.138	Block	2
37.8.86.188	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.159.165	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
79.253.50.219	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/main	Block	1
2.53.159.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
31.168.246.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
79.179.115.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/	Block	1
188.29.164.104	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.253.207.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.10.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docld in www.aka.idf.il/main/giyus/general.aspx	None	1
10.111.60.117		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
80.246.130.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.230	Netherlands	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
85.65.183.52	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.183.70.205	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
185.3.147.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
109.253.214.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
23.20.205.190	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.246.137.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ß in www.aka.idf.il/main/sachar/	None	1
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.125.230	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.125.230	Block	1
66.249.65.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/modiin/maslul.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
95.35.86.6	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.183.70.205	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1

08-18-2016-14:04:03 to 08-18-2016-15:04:03