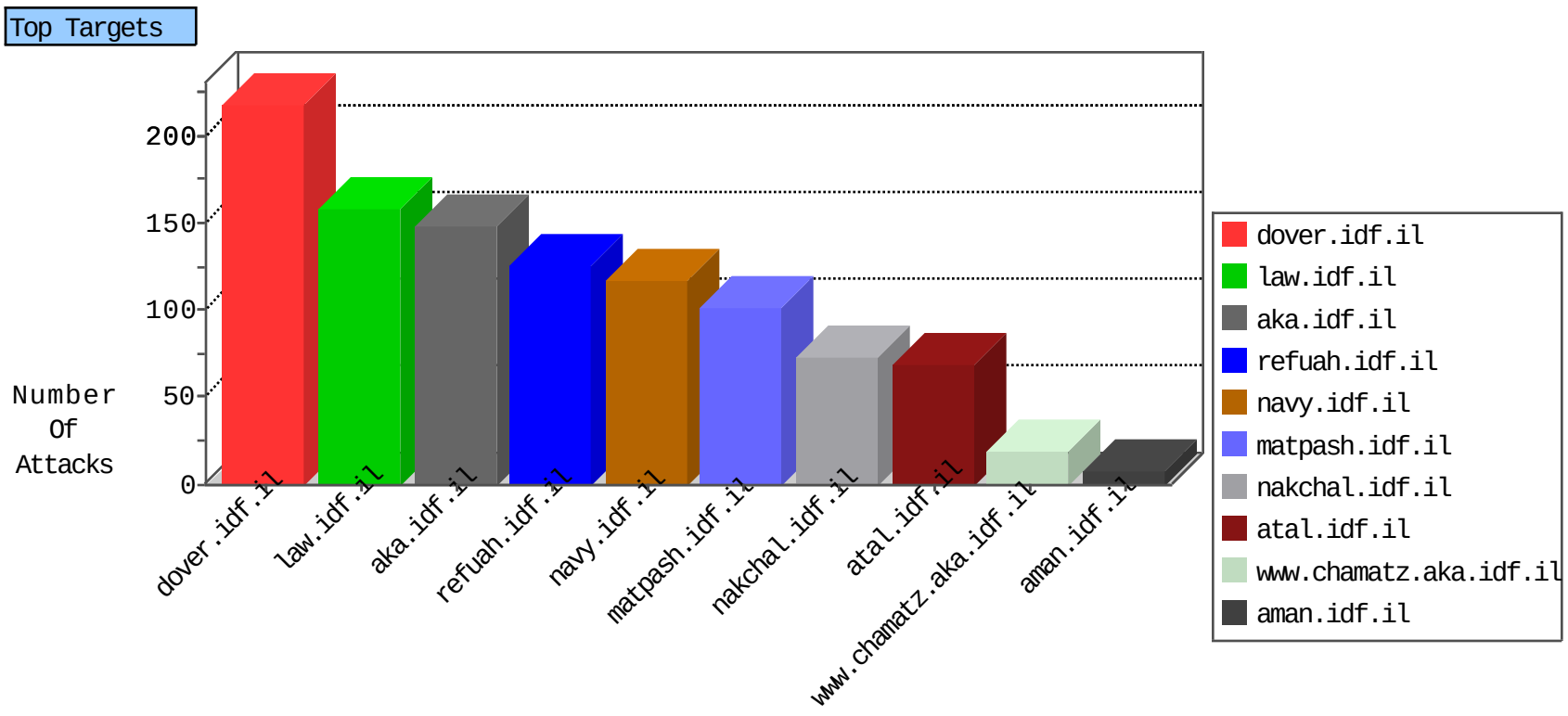
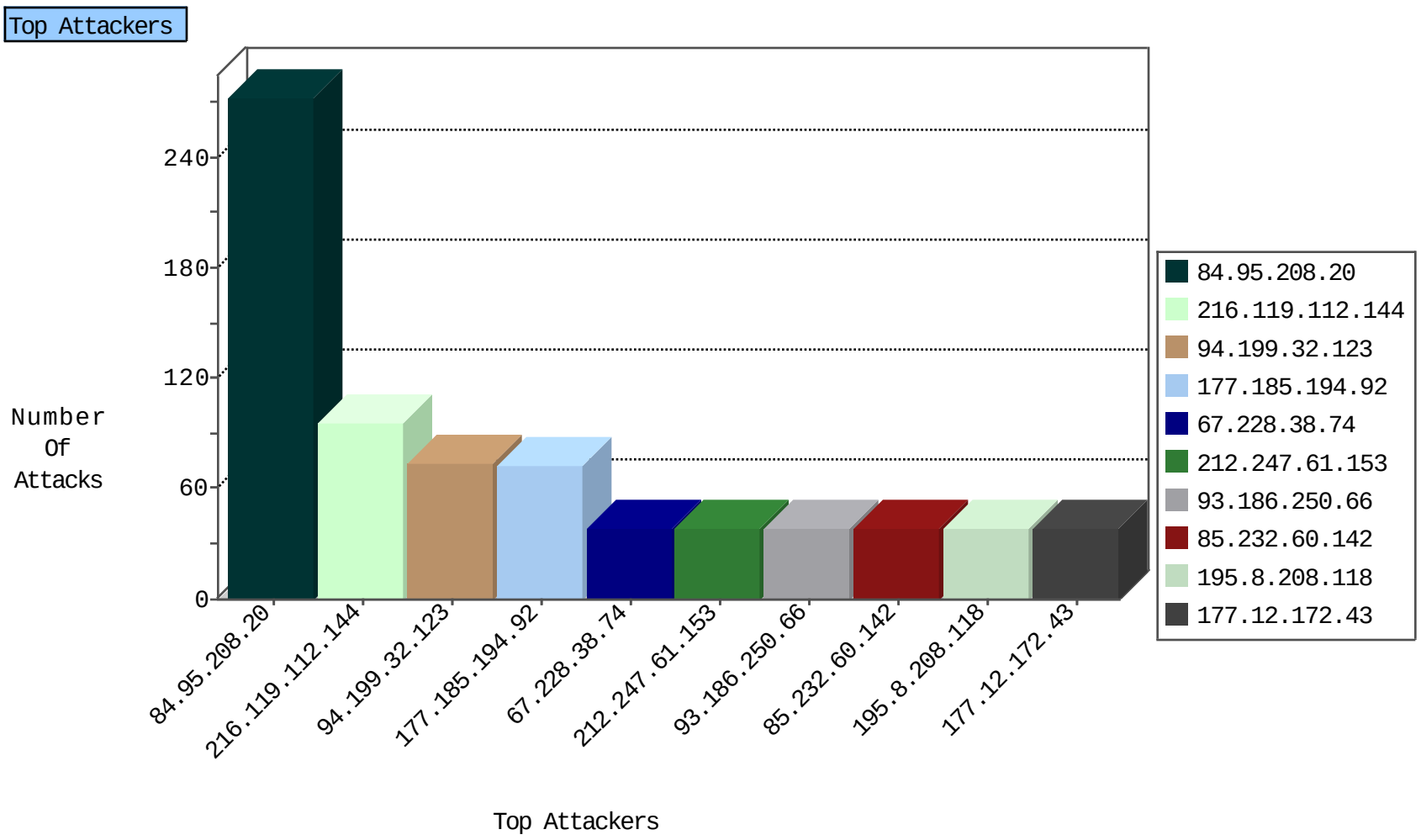
08-23-2016-02:04:04 to 08-23-2016-03:04:04

IDF Under Attack Daily Report





08-23-2016-02:04:04 to 08-23-2016-03:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.182.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
180.2.109.14	Japan	147.237.76.176	test.ncore.idf.il	Black List	drop	4
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
60.175.225.22	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
222.186.34.206	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
89.248.168.21	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-23-2016-02:04:04 to 08-23-2016-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.199.32.123	Turkey	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
83.168.250.50	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
195.8.208.118	Netherlands	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
213.174.55.11	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
85.232.60.142	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
177.185.194.92	Brazil	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
94.199.32.123	Turkey	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
212.247.61.153	Sweden	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
216.119.112.144	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
93.186.250.66	Italy	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
177.12.172.43	Brazil	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
212.247.61.153	Sweden	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
67.228.38.74	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
168.1.80.134	Australia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.232.60.142	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.92	Brazil	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
67.228.38.74	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
67.228.38.74	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.15.196.171	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
68.49.34.42	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
93.186.250.66	Italy	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.216.31	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.118	Netherlands	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
121.40.25.174	China	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.236.115.84	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.12.172.43	Brazil	147.237.76.86	navy.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
93.186.250.66	Italy	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
89.248.172.16	Netherlands	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-23-2016-02:04:04 to 08-23-2016-03:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.112.144	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	72
177.185.194.92	147.237.76.31	Brazil	nakchal.idf.il	SQL Injection - Select From	54
94.199.32.123	147.237.76.42	Turkey	refuah.idf.il	SQL Injection - Select From	38
67.228.38.74	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
177.12.172.43	147.237.76.86	Brazil	navy.idf.il	SQL Injection - Select From	20
93.186.250.66	147.237.76.42	Italy	refuah.idf.il	SQL Injection - Select From	20
212.247.61.153	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	20
85.232.60.142	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	20
195.8.208.118	147.237.76.86	Netherlands	navy.idf.il	SQL Injection - Select From	20
41.185.12.173	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	18
68.49.34.42	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
83.168.250.50	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	16
213.174.55.11	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	14
46.236.115.84	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	10
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	8
184.168.46.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
168.1.80.134	147.237.77.74	Australia	law.idf.il	SQL Injection - Select From	8
121.40.25.174	147.237.77.74	China	law.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	8
66.29.216.31	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
168.1.80.134	147.237.77.233	Australia	atal.idf.il	SQL Injection - Select From	8
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.206	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.236.194.161	147.237.72.156	Czech Republic	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.206	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.100.214.202	147.237.76.197	Australia	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1

08-23-2016-02:04:04 to 08-23-2016-03:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.185.85.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.130.6.49	Lithuania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
85.130.139.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.29.180	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
156.205.43.56	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
86.108.20.96	Jordan	147.237.77.216	dover.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
128.232.110.28	United Kingdom	147.237.0.33	idf.il	drop		drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
65.55.212.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
65.55.218.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
176.13.5.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-02:04:04 to 08-23-2016-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	132
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	9
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	7
105.225.146.58	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	5
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
213.57.154.220	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 213.57.154.220 (Open Mode)	None	1
105.102.235.88	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17615-en/dover.asp	Block	1
66.249.64.147	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
71.199.191.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
213.57.154.220	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	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
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
157.55.39.40	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
157.55.39.125	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1

08-23-2016-02:04:04 to 08-23-2016-03:04:04