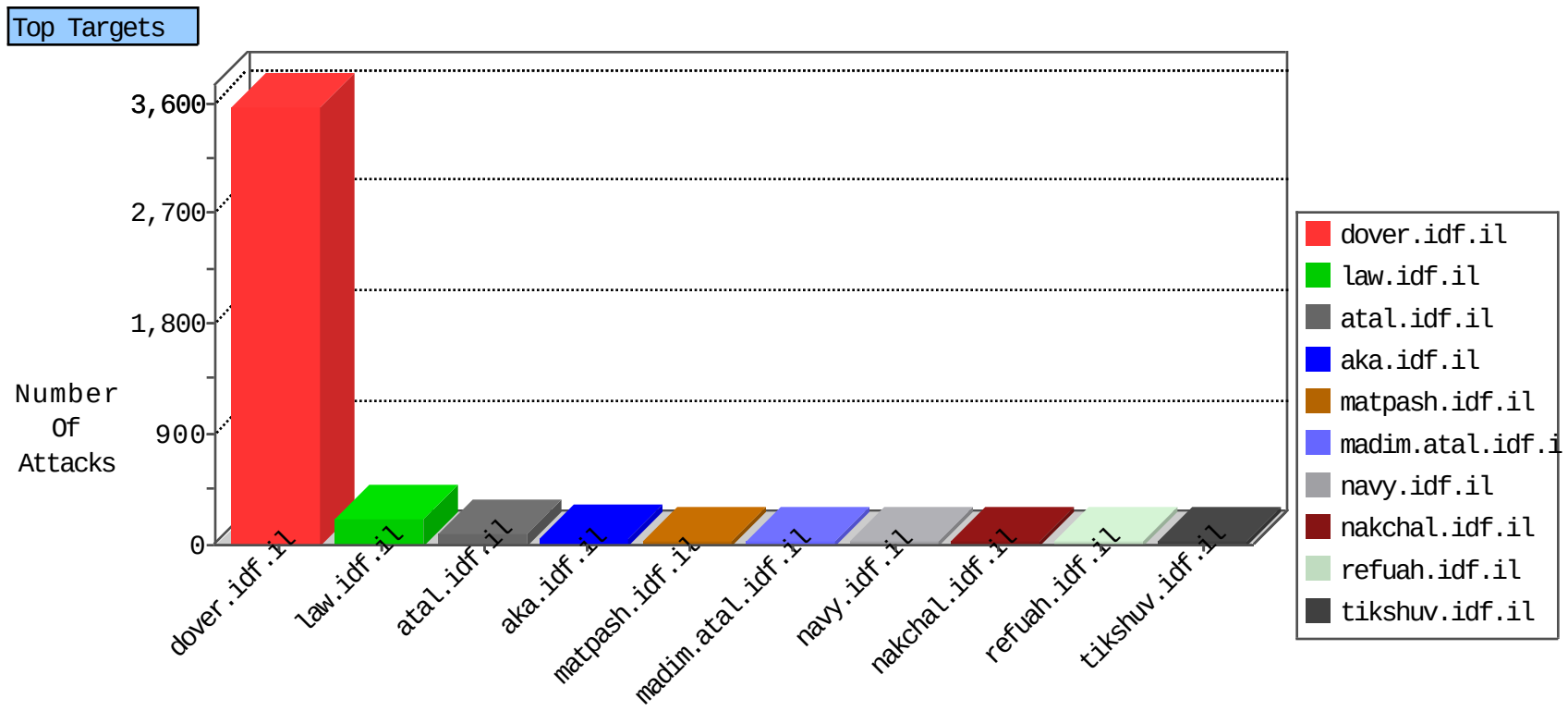
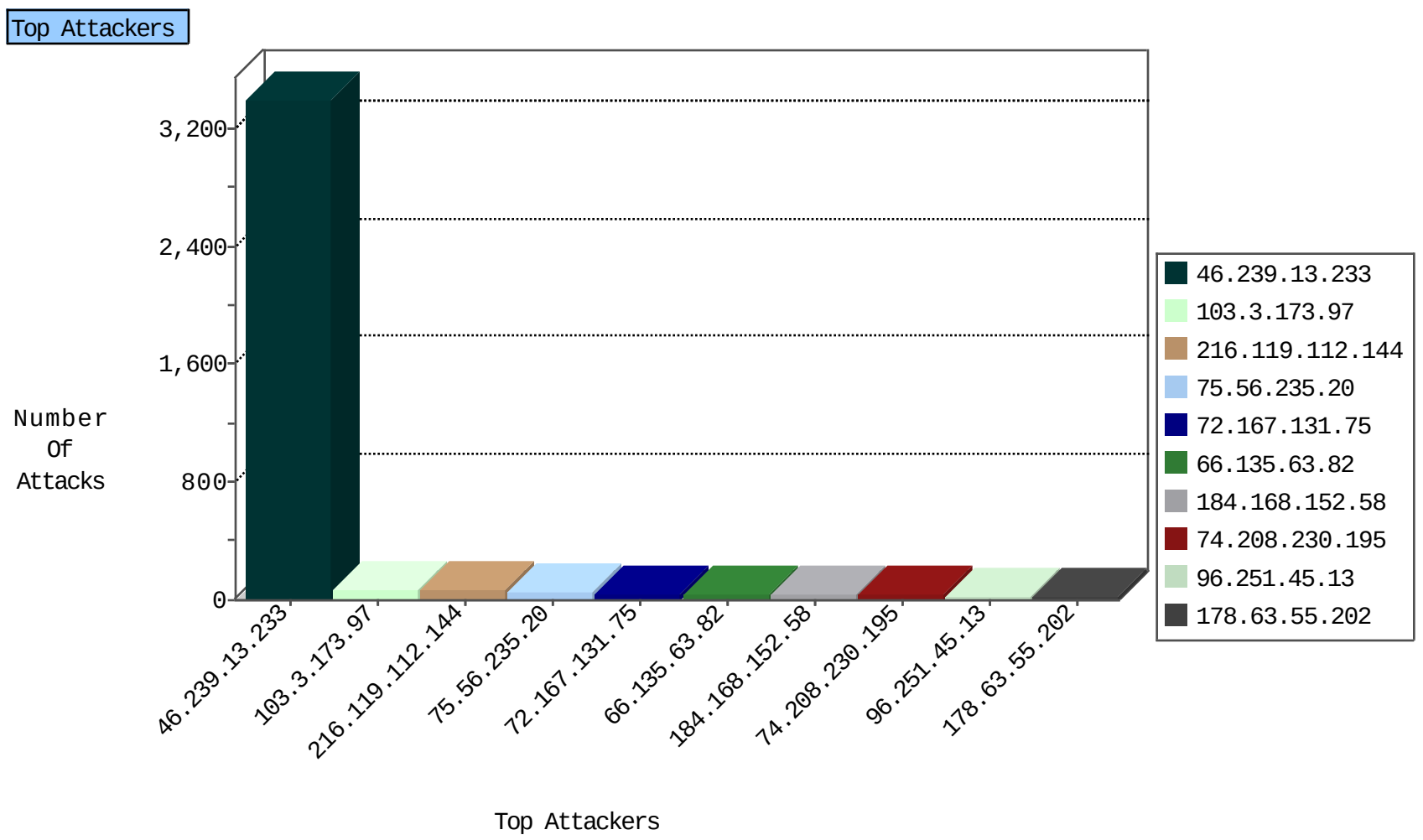
08-28-2016-23:04:05 to 08-29-2016-00:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-23:04:05 to 08-29-2016-00:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
195.246.57.38	Egypt	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	1
66.240.219.146	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
149.56.235.168	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-28-2016-23:04:05 to 08-29-2016-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.56.235.20	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
216.119.112.144	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
72.167.131.75	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
103.3.173.97	Malaysia	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.152.58	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
216.119.112.144	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.166.190.139	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.140	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
173.192.81.82	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.135.63.82	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
217.37.125.121	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.58	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.192.137	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
103.3.173.97	Malaysia	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.135.63.82	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.58	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
210.169.203.81	Japan	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.135.63.82	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
191.236.150.197	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
191.236.146.62	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
191.236.151.40	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-28-2016-23:04:05 to 08-29-2016-00:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.112.144	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	54
103.3.173.97	147.237.77.216	Malaysia	dover.idf.il	SQL Injection - Select From	54
75.56.235.20	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	36
66.135.63.82	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
184.168.152.58	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
72.167.131.75	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
173.192.81.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.208.192.137	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
108.166.190.139	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
87.242.112.45	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
217.37.125.121	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
74.208.230.195	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	8
210.169.203.81	147.237.72.166	Japan	aka.idf.il	SQL Injection - Select From	8
50.63.197.140	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
87.115.230.45	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
191.236.150.197	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	2
87.115.230.45	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
94.102.48.195	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
159.203.33.10	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
137.117.168.203	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.76.197	Mexico	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
123.206.73.185	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
106.187.90.86	147.237.0.33	Japan	idf.il	GPL SCAN superscan echo	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
137.117.168.203	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.76.197	Mexico	e.himush.idf.il	ET SCAN NMAP -f -sS	1
109.66.190.248	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
191.236.151.40	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	1
106.187.90.86	147.237.0.200	Japan	m4u.idf.il	GPL SCAN superscan echo	1
191.236.146.62	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	1

08-28-2016-23:04:05 to 08-29-2016-00:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3398
96.251.45.13	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
74.208.230.195	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	24
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
67.174.112.111	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
212.247.61.153	Sweden	147.237.72.156	aman.idf.il	drop	SAM rule	drop	12
177.185.194.45	Brazil	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
46.120.122.219	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	11
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
91.219.122.4	Poland	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
46.236.115.84	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
83.168.250.50	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
213.246.49.11	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
84.152.1.112	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.122.219	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
207.46.13.111	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
176.13.224.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.159.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.44.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
208.80.192.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.109.213.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.84.77.34	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
1.192.128.23	China	147.237.76.34	yohalan.idf.il	drop		drop	1
138.246.253.19	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.3.42	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
89.22.178.162	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.3.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
137.117.168.203	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.120.122.219	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1

08-28-2016-23:04:05 to 08-29-2016-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.26.224	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	9
176.13.226.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
216.244.66.242	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.51.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.230.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.143.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
109.253.208.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.235	Block	1
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
109.66.50.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22717-he/dover.aspx	Block	1
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method T_SessionId=3cumydttu3mmyeyf12s3wblg in URL	Block	1
1.192.128.23	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/manager/html	Block	1
79.178.4.96	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/kidsfromgaza.aspx	Block	1
46.19.86.83	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.230	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.69.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/modiin/general.aspx	Block	1
77.127.57.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.69.145	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
2.53.158.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
87.69.93.89	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation SearchText in www.logistics.atal.idf.il/938-he/halag.aspx	Block	1
66.249.69.229	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
46.121.69.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
213.8.204.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.93.89	Israel	147.237.77.234	halag.idf.il	Suspicious Response Code	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/shalishut/site/general.aspx	None	1
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
1.192.128.23	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/manager/html	Block	1
172.56.5.129	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
77.139.201.200	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1

08-28-2016-23:04:05 to 08-29-2016-00:04:05