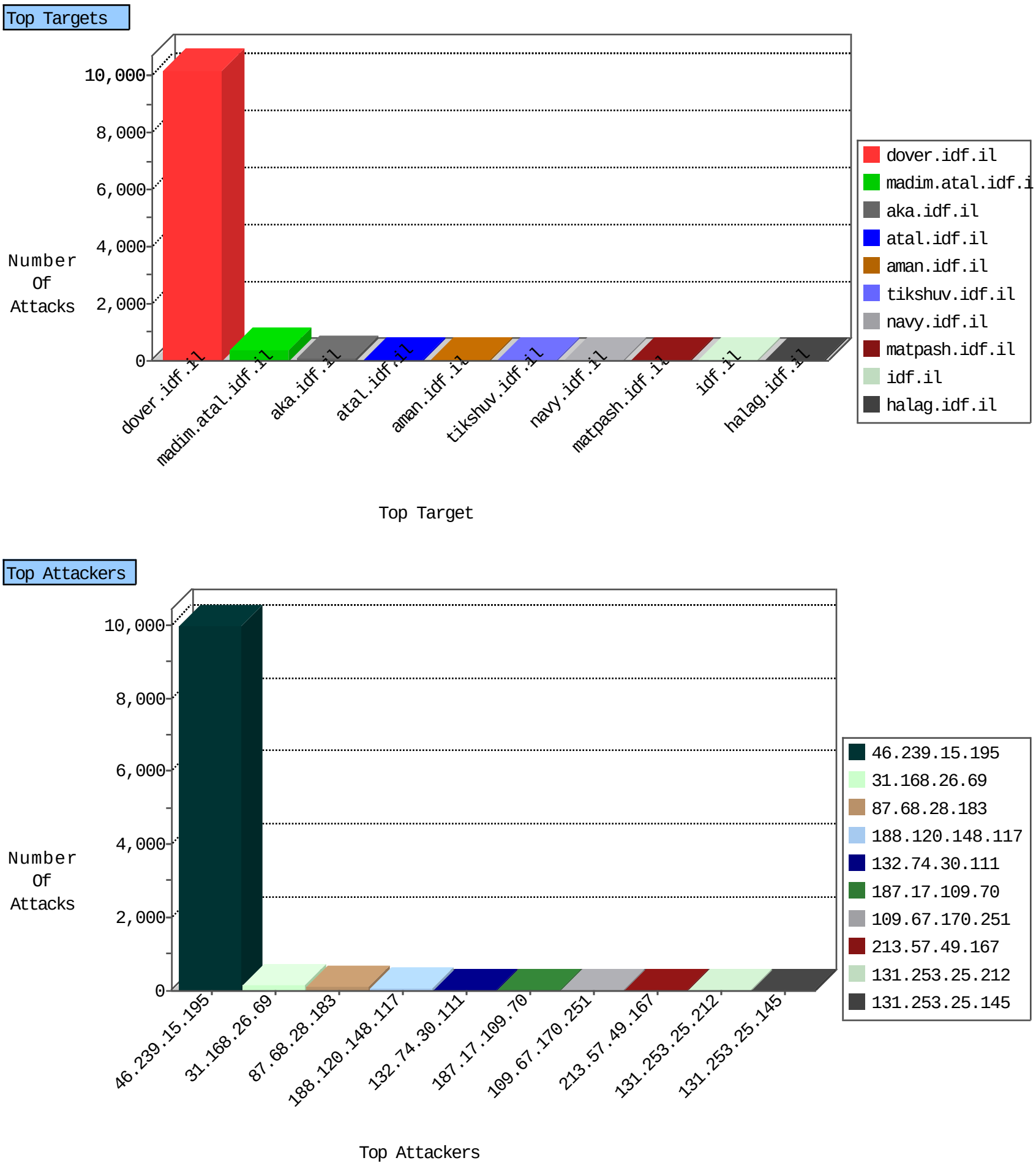
08-27-2016-12:04:04 to 08-27-2016-13:04:04

IDF Under Attack Daily Report



08-27-2016-12:04:04 to 08-27-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	4
2.53.139.228	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
116.241.167.209	Taiwan	147.237.76.202	e.halag.idf.i	Black List	drop	2

08-27-2016-12:04:04 to 08-27-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.17.109.70	Brazil	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
187.17.109.70	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.8.24.172	Israel	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
51.255.65.41	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-27-2016-12:04:04 to 08-27-2016-13:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
187.17.109.70	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	20
213.8.24.172	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	8
182.254.131.170	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
163.172.195.167	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.195.167	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
85.214.26.80	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.195.167	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.239.15.195	147.237.77.216	Bosnia and Herzegovina	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.195.167	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.195.167	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.195.167	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
201.238.202.219	147.237.72.14	Chile	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
85.214.26.80	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1

08-27-2016-12:04:04 to 08-27-2016-13:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9411
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	597
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
2.55.55.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
46.119.116.73	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.247.61.153	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
66.102.9.185	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
203.133.171.21	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.65.62.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.239.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop		drop	2
68.180.230.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop		drop	2
183.129.160.229	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
40.77.169.101	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
131.253.25.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.104	United States	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
183.129.160.229	China	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
49.148.208.108	Philippines	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	1
141.212.122.68	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
38.229.1.15	United States	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.69	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.33	idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.251.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
109.253.204.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.26.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
87.68.28.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
188.120.148.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
132.74.30.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
131.253.25.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	23
131.253.25.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	23
109.67.170.251	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	19
109.186.90.255	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	14
109.67.170.251	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.170.251	Block	14
131.253.27.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.176.75.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.23.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.46.41.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1538	Block	2
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
46.116.2.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.108.180.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1236-he/atal.aspx	Block	1
176.228.201.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
77.138.45.57	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
65.55.212.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.26.248	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.86.66	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.204.108.16	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
109.67.170.251	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/	Block	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.10	Block	1
87.69.239.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
207.46.13.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
40.77.169.97	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.177.4.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files	Block	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
40.77.169.102	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /351-en/patzar.aspx#011404	Block	1
93.157.84.34	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.63.85	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/search/results.aspx	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.117.195.51	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.199.242	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

08-27-2016-12:04:04 to 08-27-2016-13:04:04