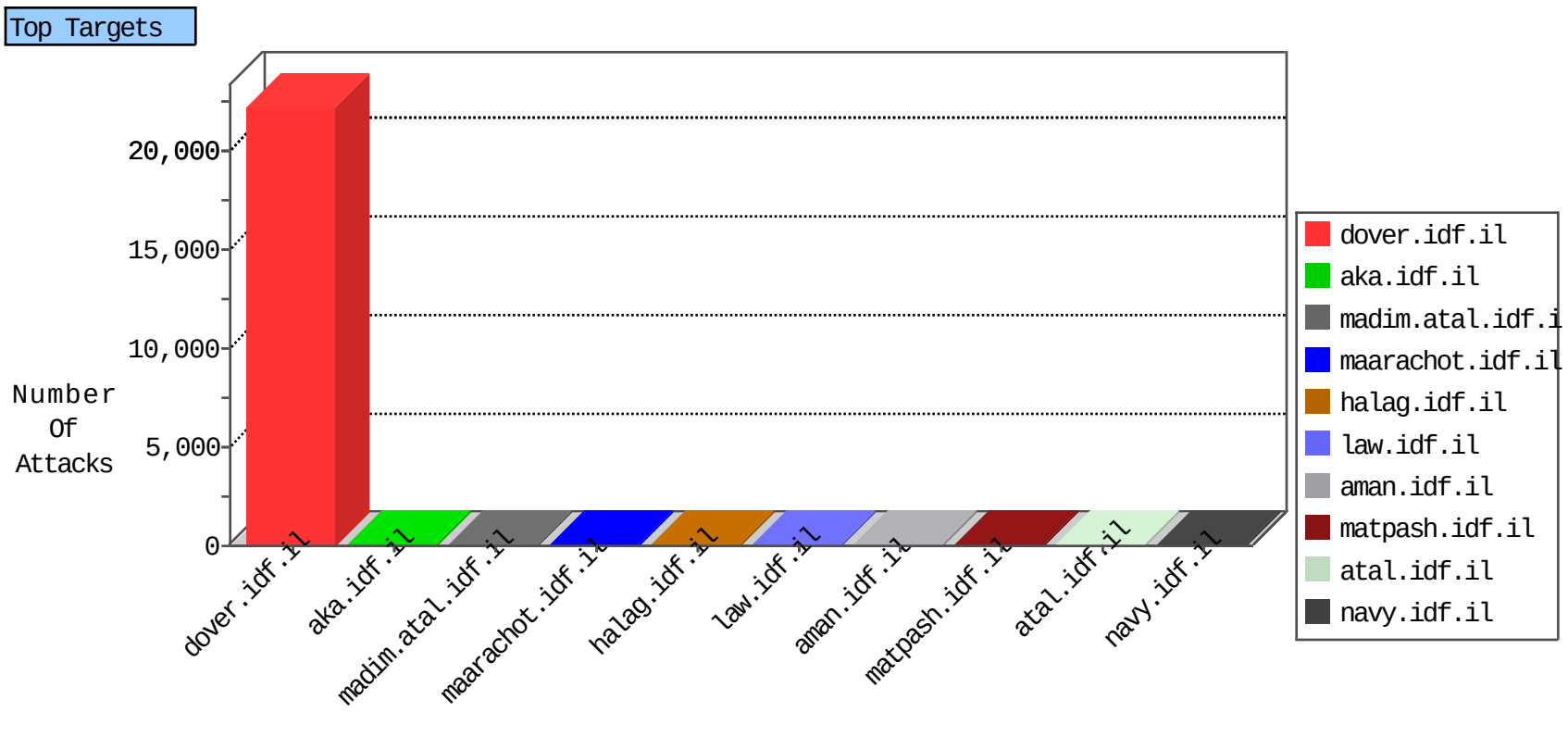
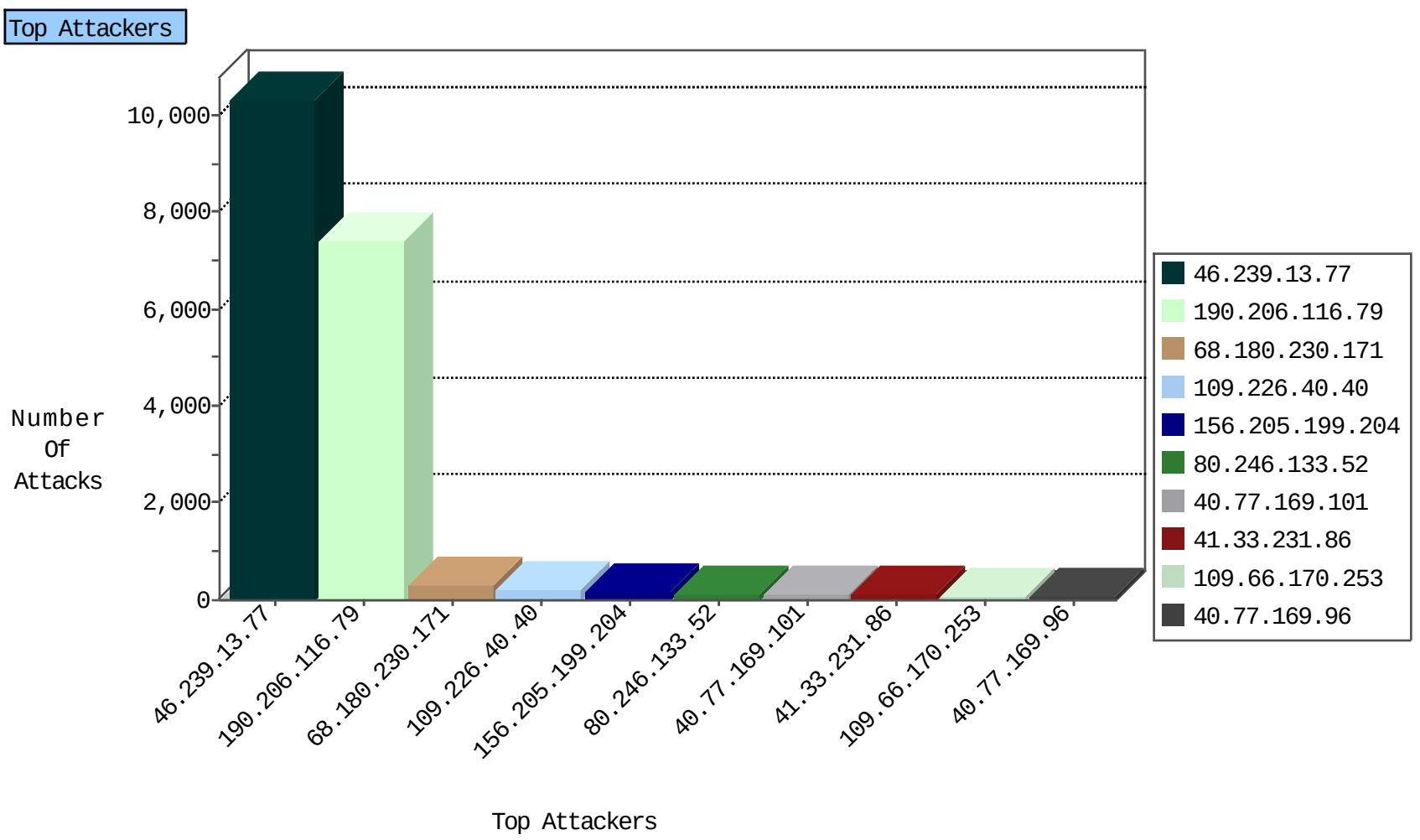
08-26-2016-20:04:04 to 08-26-2016-21:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-20:04:04 to 08-26-2016-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	129572
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22185
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	22102
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	16443
104.152.52.68	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	231
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	190
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	185
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	118
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	108
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	92
80.246.133.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	85
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	64
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	62
66.249.76.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	47
40.77.169.96	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	46
80.246.133.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
66.249.66.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	37
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
109.66.170.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
89.138.196.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
109.66.170.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
66.249.76.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
109.253.130.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
109.253.212.247	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
109.65.32.101	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
209.216.220.70	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
45.33.129.87	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
109.67.0.121	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
40.77.169.102	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
94.230.86.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
89.138.157.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
40.77.169.99	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
46.117.132.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
37.26.146.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
109.253.130.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
70.193.20.142	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
104.152.52.68	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
40.77.167.36	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
40.77.169.96	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
176.13.16.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15

08-26-2016-20:04:04 to 08-26-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.151.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.206	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-26-2016-20:04:04 to 08-26-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
27.254.130.46	147.237.76.38	Thailand	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.199	Moldova, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.197	Moldova, Republic of	e.himush.idf.il	ET SCAN Potential SSH Scan	1
123.206.85.139	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
27.254.130.46	147.237.76.197	Thailand	e.himush.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.202	Moldova, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
27.254.130.46	147.237.76.30	Thailand	himush.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.107	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.76.148	Sweden	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1

08-26-2016-20:04:04 to 08-26-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10186
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	493
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	72
190.79.229.218	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
41.141.6.247	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
77.125.11.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.98	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	7
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
46.19.85.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
64.87.23.55	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
109.253.157.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
87.68.18.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.67.65	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
37.76.211.238	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.151.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
40.77.169.101	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	3
94.230.86.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
37.46.39.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.245	Israel	147.237.77.216	dover.idf.il	drop		drop	2
46.19.85.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.111.136.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.90.164.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.150.73	Israel	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
176.13.21.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.168.51.225	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
109.66.15.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.102.9.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
84.108.66.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
59.180.241.133	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.179.215.182	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

08-26-2016-20:04:04 to 08-26-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.237.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
85.65.131.172	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.131.172	Block	14
79.181.130.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.130.2	Block	10
79.179.182.59	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	6
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	3
93.171.142.242	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.27.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.53.14.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
187.160.231.76	Mexico	147.237.77.226	www.chamatz.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
85.64.234.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.110	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
40.77.169.99	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
121.34.160.11	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
189.215.82.53	Mexico	147.237.76.39	mobile.meitav.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.181.130.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/register.asp	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
189.215.82.53	Mexico	147.237.76.42	refuah.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
85.65.131.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kios/kiosk.aspx	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
189.219.172.64	Mexico	147.237.77.170	maarachot.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
79.179.182.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
41.141.6.247	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
187.160.85.12	Mexico	147.237.77.74	law.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
66.249.66.213	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/mobile/	Block	1
201.173.82.23	Mexico	147.237.76.147	chinuch.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
37.76.211.238	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
121.34.160.11	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.34.160.11	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1

08-26-2016-20:04:04 to 08-26-2016-21:04:04