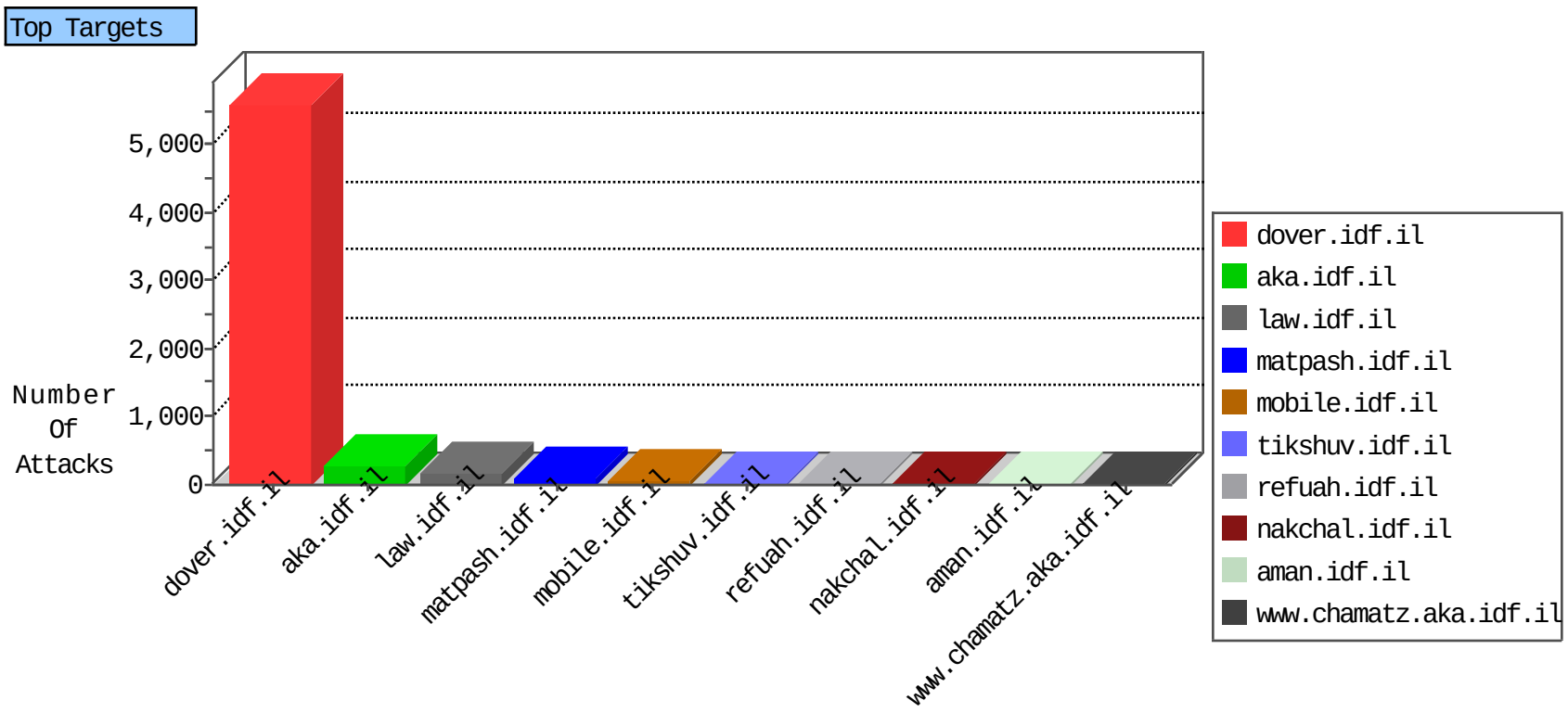
10-28-2015-00:04:09 to 10-28-2015-01:04:09

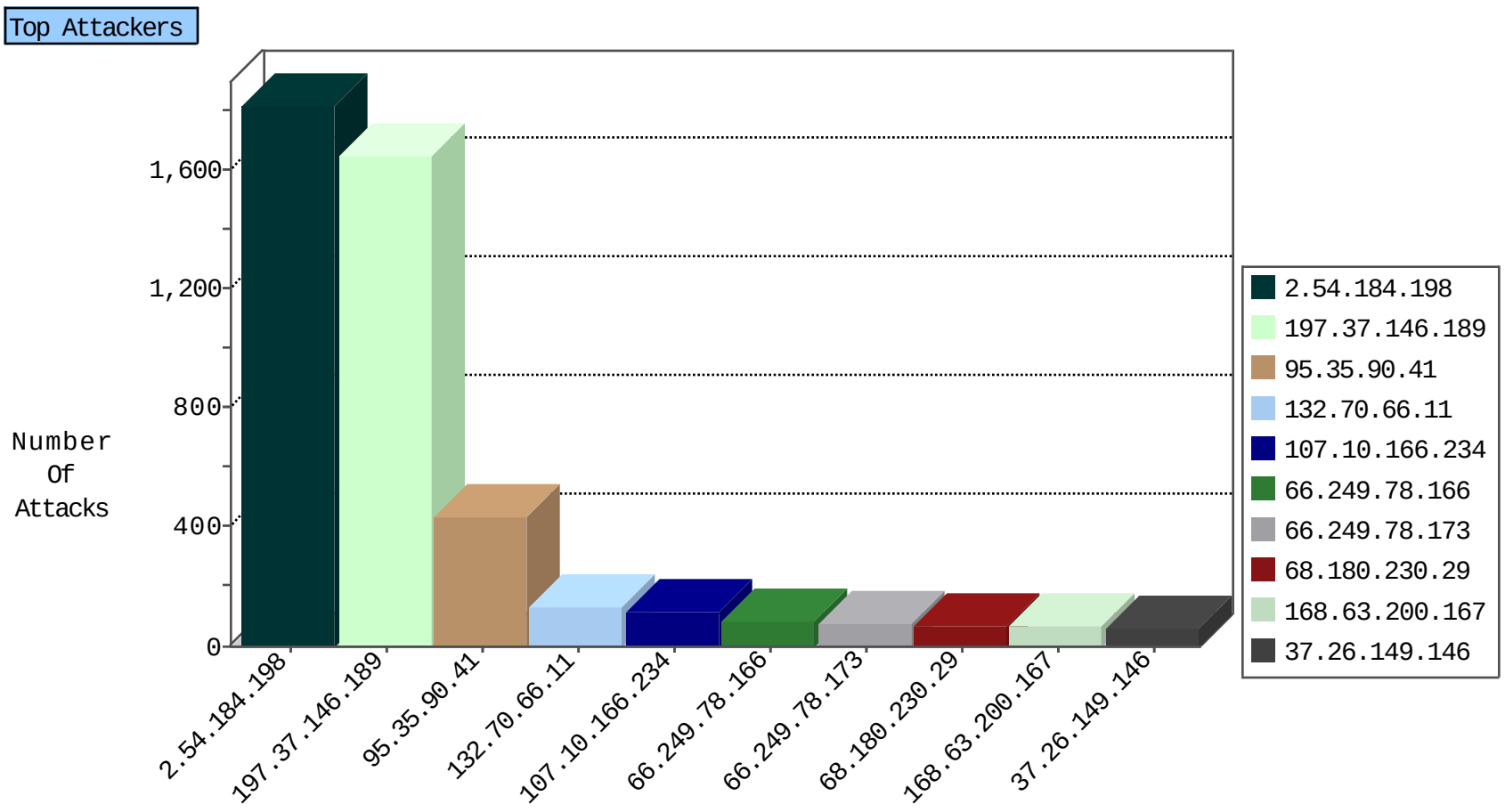
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-28-2015-00:04:09 to 10-28-2015-01:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.149.234	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	28
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	23
89.134.59.16	Hungary	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
81.218.33.77	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
2.54.32.112	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.85.202	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
2.54.61.117	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.85.220	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
185.19.223.60	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4
149.78.163.150	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	4
149.78.163.150	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	4
87.69.171.67	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
100.100.47.54		147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	2
46.19.85.220	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
109.67.3.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
46.19.86.78	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
31.168.221.125	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
99.11.90.249	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
46.19.85.220	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	1
46.19.85.202	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	1

10-28-2015-00:04:09 to 10-28-2015-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.52.100	Germany	147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	11
149.202.52.100	Germany	147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

10-28-2015-00:04:09 to 10-28-2015-01:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
51.36.34.58	147.237.77.216	United Kingdom	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
217.219.67.177	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.52.100	147.237.76.31	Germany	nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
89.248.171.19	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -f -sS	1
217.219.67.177	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
193.105.134.220	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.171.19	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.19	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

10-28-2015-00:04:09 to 10-28-2015-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.184.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1819
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1523
95.35.90.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	432
132.70.66.11	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	133
107.10.166.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
168.63.200.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
37.26.149.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
5.110.35.181	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop		drop	57
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.117.254.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.62.5.158	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
197.247.179.48	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.142.191.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.114.110		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.60.168		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.12.136.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
69.156.119.252	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.64.115.32	Israel	147.237.76.31	nakchal.idf.i	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
82.145.209.91	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
188.120.148.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.186.183.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.120.148.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.66.179.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-28-2015-00:04:09 to 10-28-2015-01:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	70
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
2.54.148.50	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
84.228.87.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
176.106.227.95	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
176.106.227.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
84.228.87.189	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
62.182.209.210	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/7/1557.jpg	Block	14
188.40.122.149	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 188.40.122.149	Block	14
40.77.167.42	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	14
176.13.14.93	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	14
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	14
95.86.106.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sa in www.aka.idf.il/main/smalim/smalim.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/history/in_mivzaim.asp	Block	14
45.63.49.95		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	14
207.46.13.181	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	14
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
188.165.15.60	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
99.11.90.249	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.19.86.78	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	14
84.110.34.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	14
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english.	Block	14
46.117.61.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
213.57.176.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
180.76.15.10	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	14
31.168.221.125	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.37.146.189	Block	14
168.235.194.141	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.pngimg /	Block	14
67.79.31.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	14

10-28-2015-00:04:09 to 10-28-2015-01:04:09