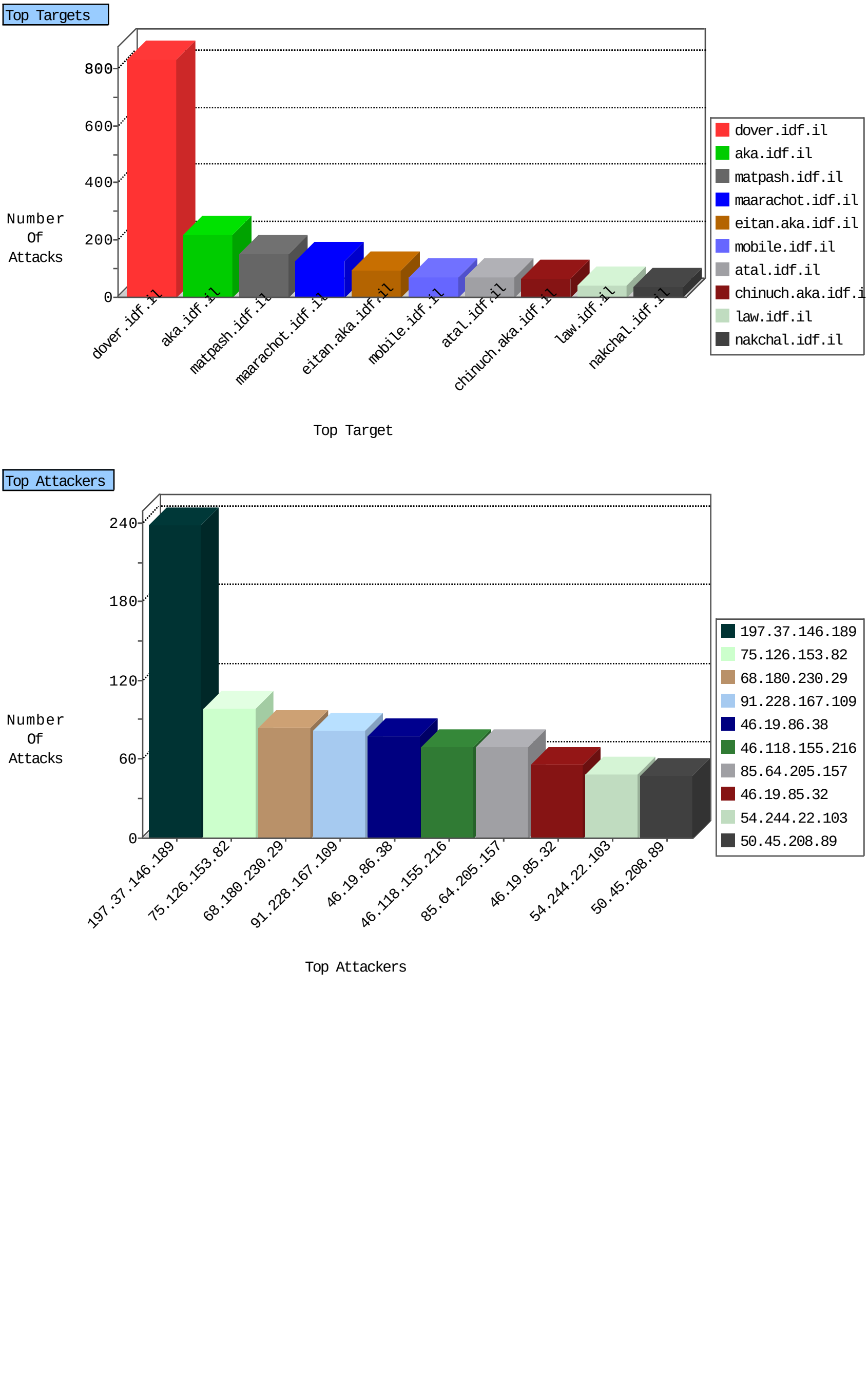
10-28-2015-01:04:06 to 10-28-2015-02:04:06

IDF Under Attack
Daily Report



10-28-2015-01:04:06 to 10-28-2015-02:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.45.208.89	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
213.57.224.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
79.177.162.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
188.247.78.165	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
96.35.50.133	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
183.60.48.25	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
2.52.19.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.52.164.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-28-2015-01:04:06 to 10-28-2015-02:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-28-2015-01:04:06 to 10-28-2015-02:04:06

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	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
89.248.162.130	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
199.101.186.134	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
185.100.84.253	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
112.162.204.84	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
75.126.153.82	147.237.77.170	United States	maarachot.idf.il	SERVER-WEBAPP admin.php access	1
1.29.13.30	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-28-2015-01:04:06 to 10-28-2015-02:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.19.86.38	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop		drop	45
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	40
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
179.230.133.132	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
132.70.66.11	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	36
50.45.208.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	34
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	20
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.26.149.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
131.253.25.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.192.68.46	Netherlands	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	10
213.57.224.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.164.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.19.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	7
31.210.187.244	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	7
87.69.166.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.164.93.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
96.35.50.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
164.76.68.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
75.73.178.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.157.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.177.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.162.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
88.81.34.114	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
76.219.112.206	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.142.193.90	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.160.133.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.223.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.69.90.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

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/2113-he/cogat.aspx	Block	84
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.205.157	Block	56
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	42
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
2.52.19.96	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	28
75.126.153.82	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	28
75.126.153.82	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 75.126.153.82	Block	28
75.126.153.82	United States	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	28
66.249.79.106	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
217.69.133.230	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	14
141.212.122.160	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	14
66.249.74.93	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	14
207.46.13.155	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.32	Block	14
85.250.151.86	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	14
2.54.18.176	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.18.176 (Open Mode)	None	14
149.78.38.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	14
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	14
207.46.13.181	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/skira/default.asp	None	14
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.32	Block	14
85.250.151.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	14
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	14
157.55.39.177	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	14
2.54.18.176	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
75.126.153.82	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	14
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	14
212.129.31.47	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.32	Block	14
109.64.134.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
174.51.65.57	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	14
2.54.52.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.79.104	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.32	Block	14
212.129.31.47	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	14
109.65.177.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.37.146.189	Block	14
37.147.211.108	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	14
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13

10-28-2015-01:04:06 to 10-28-2015-02:04:06