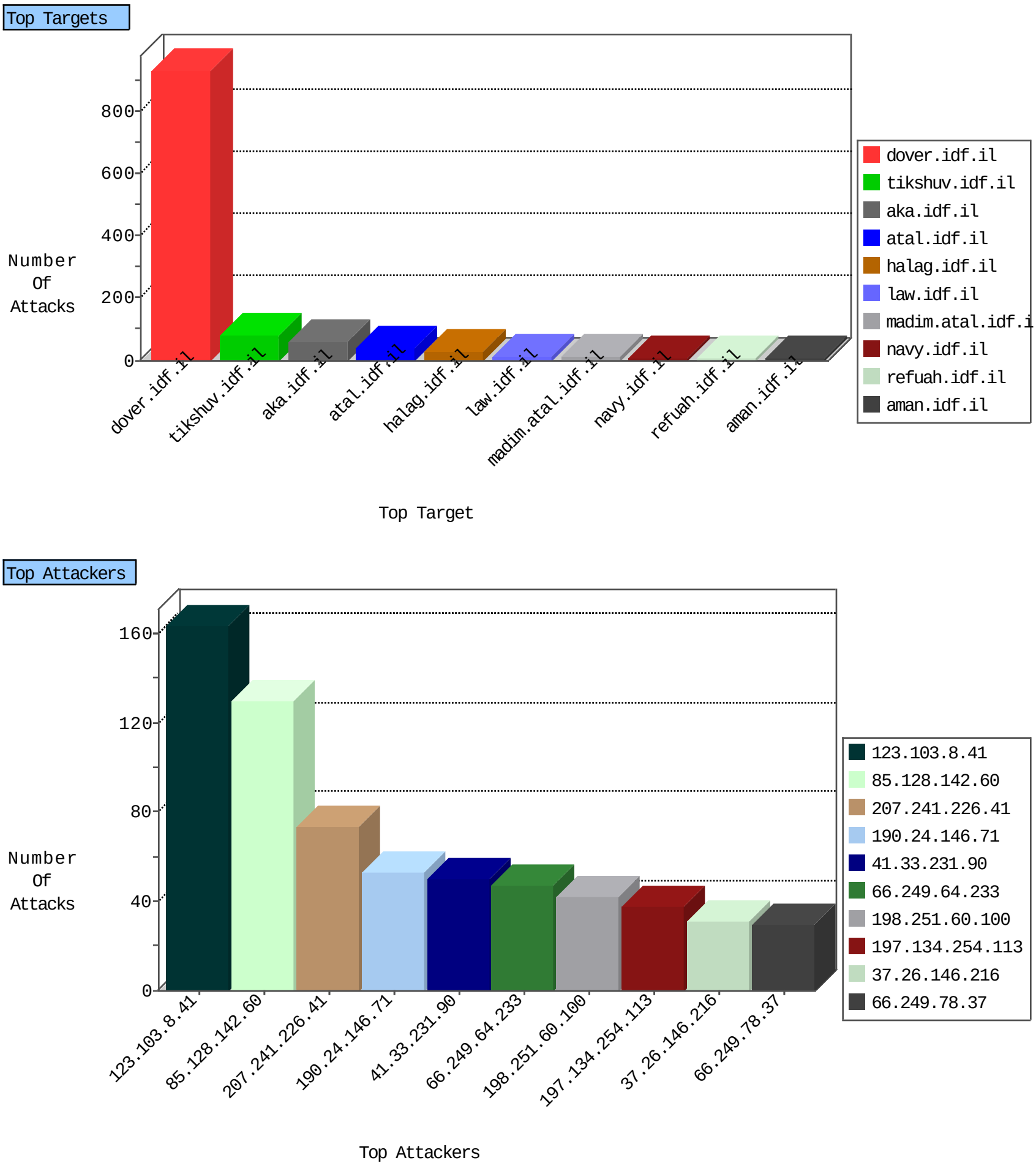
11-23-2015-01:06:18 to 11-23-2015-02:06:18

IDF Under Attack
Daily Report



11-23-2015-01:06:18 to 11-23-2015-02:06:18

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5923
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3319
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
142.4.193.203	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.12.12.164	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

11-23-2015-01:06:18 to 11-23-2015-02:06:18

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-23-2015-01:06:18 to 11-23-2015-02:06:18

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
173.224.117.166	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
173.224.117.166	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.166	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.108.21.16	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
90.44.93.107	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
194.72.112.130	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
77.109.38.223	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
175.253.28.211	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.27.33.12	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.224.117.166	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.166	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.108.21.16	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.108.21.16	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
90.44.93.107	147.237.76.44	France	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
194.72.112.130	147.237.0.19	United Kingdom	madim.atal.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
90.44.93.107	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	1
194.72.112.130	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
31.168.172.146	147.237.77.179	Israel	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
173.224.117.166	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.166	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1

11-23-2015-01:06:18 to 11-23-2015-02:06:18

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.128.142.60	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
123.103.8.41	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
198.251.60.100	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
123.103.8.41	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
197.134.254.113	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.26.146.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
52.34.29.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.22.131.214	Denmark	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	16
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
63.249.66.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
80.246.130.86	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.130.86	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
79.183.187.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.205.108.100	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
89.128.35.163	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.36.74.228	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.121.40.123	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.198.25.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.228.54.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.22.12		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.129.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
183.79.223.92	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
209.133.111.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.8.82.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.146.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
70.187.168.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

11-23-2015-01:06:18 to 11-23-2015-02:06:18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	74
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.126.163.232	Block	5
84.108.235.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.235.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
37.142.111.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
174.89.80.210	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.7.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
52.23.156.32	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.68.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.88.182	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter p in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
176.228.54.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
124.73.1.18	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 124.73.1.18	Block	1
87.69.38.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
204.93.154.201	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.45.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
124.73.1.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/925-he/cogat.aspx/trackback/	Block	1
87.69.105.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.186.194	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.179.107.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.93.154.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
2.54.174.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.143.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

11-23-2015-01:06:18 to 11-23-2015-02:06:18