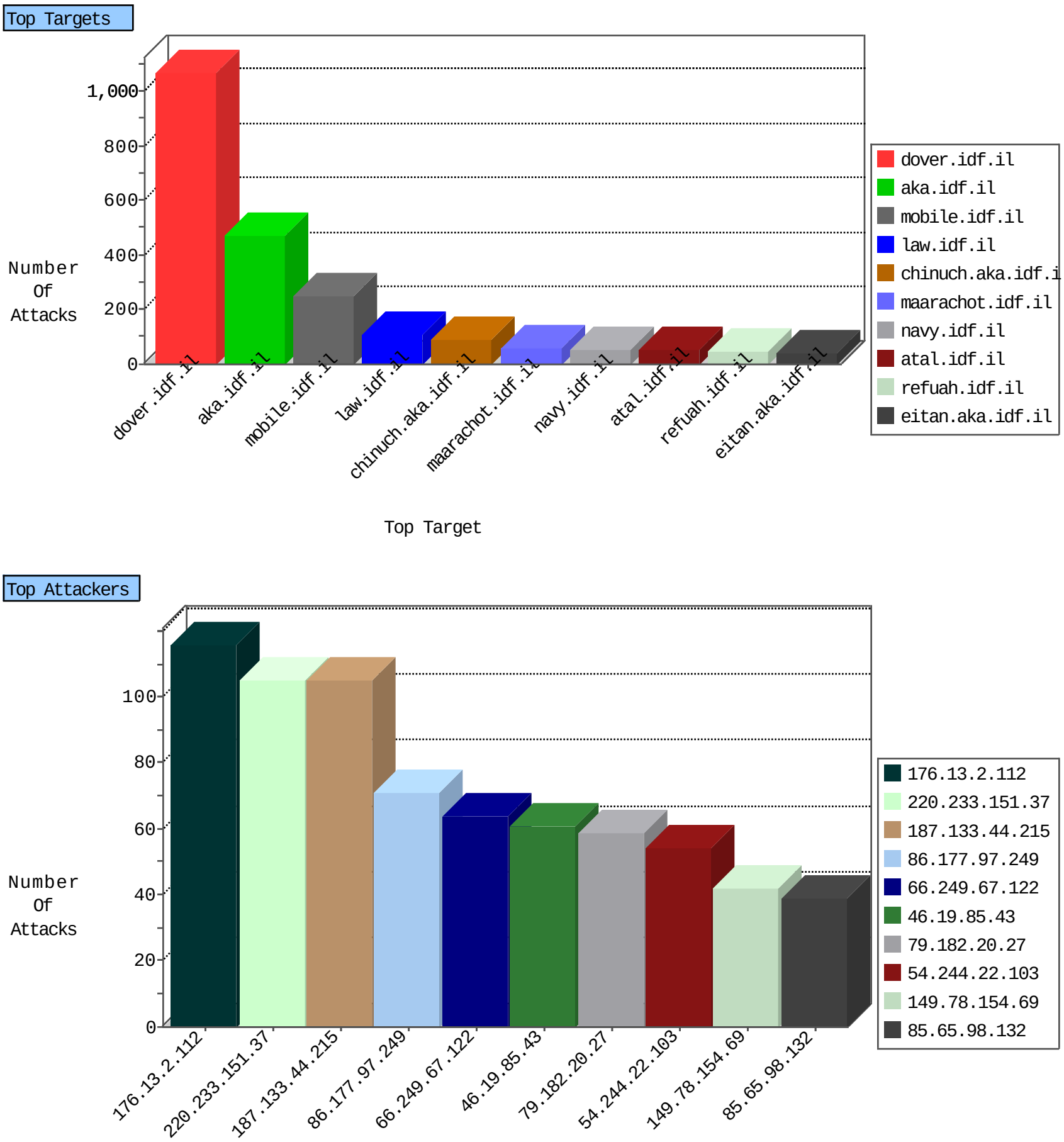
10-30-2015-01:04:02 to 10-30-2015-02:04:02

IDF Under Attack
Daily Report



10-30-2015-01:04:02 to 10-30-2015-02:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.54.248.209	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1874
198.58.103.102	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	675
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	339
157.55.39.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	268
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	92
176.13.20.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.172.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.148.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
74.117.133.194	United States	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
186.223.19.60	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
46.101.3.227	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
176.12.141.240	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
23.239.69.234	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

10-30-2015-01:04:02 to 10-30-2015-02:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-30-2015-01:04:02 to 10-30-2015-02:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.67.25	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
74.117.133.194	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.183.219.66	147.237.76.30	Latvia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
118.244.216.171	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
117.21.174.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.219.66	147.237.76.44	Latvia	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.219.66	147.237.72.14	Latvia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
118.244.216.171	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

10-30-2015-01:04:02 to 10-30-2015-02:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
86.177.97.249	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
46.19.85.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
79.182.20.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
85.65.98.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
176.13.2.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.68.188.59	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.75.38	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
168.63.139.43	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
93.172.191.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.75.46	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.20.1		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
122.56.185.177	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.244.119.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.43.30		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
172.56.8.241	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
49.224.101.224	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.1.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.182.52.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
96.54.248.209	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.15.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.244.118.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.86.113.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.121.80.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.75.30	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.102.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.113.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

10-30-2015-01:04:02 to 10-30-2015-02:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.133.44.215	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	105
176.13.2.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
220.233.151.37	Australia	147.237.77.74	law.idf.il	PHP Attempt	Block	45
220.233.151.37	Australia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	30
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	30
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
176.13.1.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	29
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
157.55.39.183	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
88.150.221.120	United Kingdom	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	15
37.142.242.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/faq.aspx	Block	15
176.13.20.191	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1152-he/chinuch.aspx	Block	15
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/925-he/refuah.aspx	Block	15
109.160.167.234	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	15
66.249.79.119	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1769	Block	15
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	15
188.165.15.241	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
88.150.221.120	United Kingdom	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	15
49.204.115.89	India	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	15
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/klali.aspx	Block	15
185.32.179.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/112274.pdf	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	15
109.160.235.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
2.52.38.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	15
220.233.151.37	Australia	147.237.77.74	law.idf.il	Admin Blocking	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
88.198.26.84	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 88.198.26.84	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/templates/album.aspx	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71800-he/maarachot.aspx	Block	15
109.160.235.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
79.177.197.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
8.37.70.143	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx&usg=alkjrhjoe2lvbuv4fpbnkgrnrjauzy0_ew	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1248-he/atal.aspx	Block	15
220.233.151.37	Australia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 220.233.151.37	Block	15
176.13.2.112	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
89.218.97.60	New Zealand	147.237.77.216	dover.idf.il	Admin Blocking	Block	15
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	15
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1139-he/atal.aspx	Block	15
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/108054.pdf	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/thumb.jpg	Block	15
87.69.105.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15

10-30-2015-01:04:02 to 10-30-2015-02:04:02