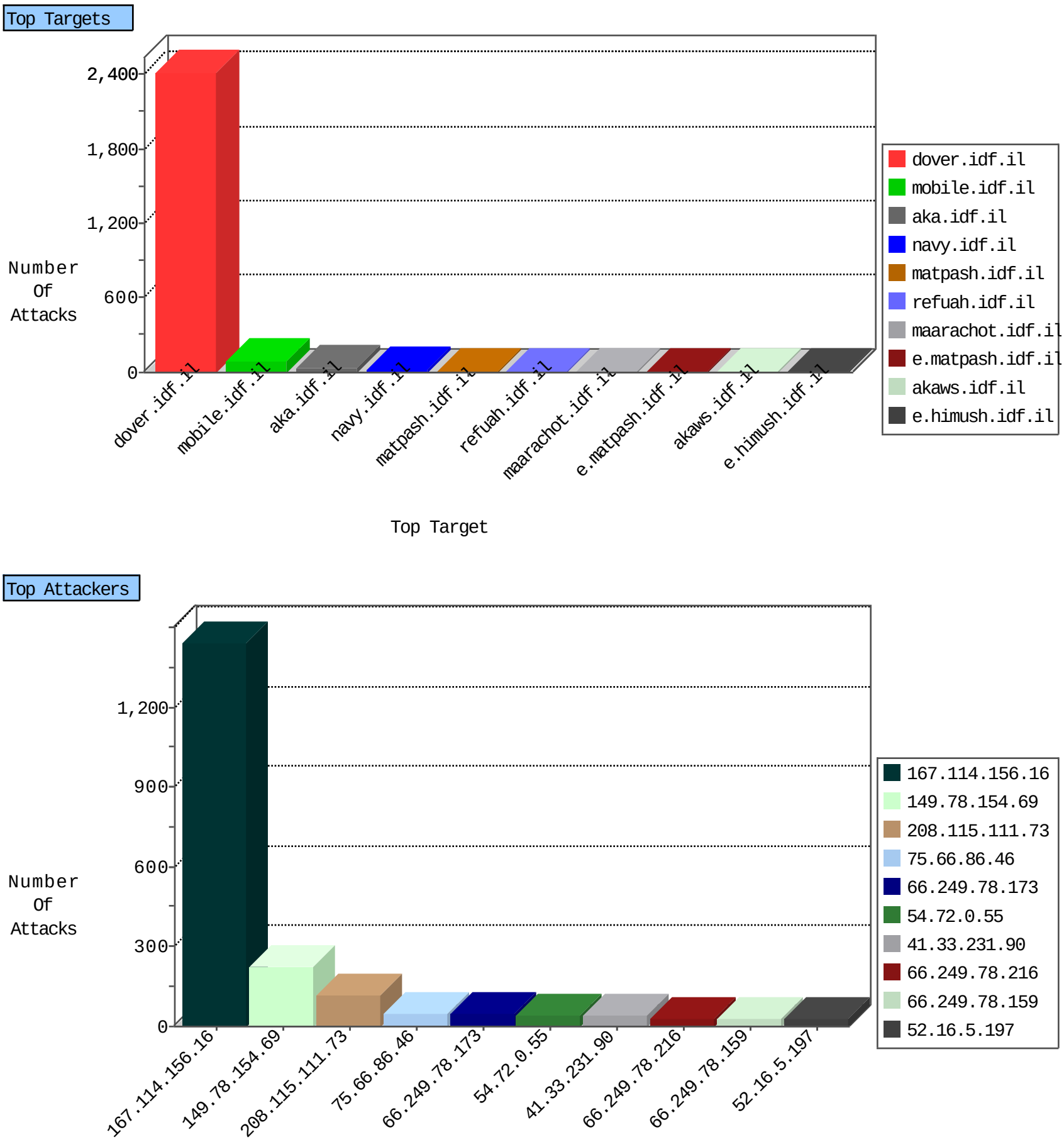
11-03-2015-04:04:07 to 11-03-2015-05:04:07

IDF Under Attack
Daily Report



11-03-2015-04:04:07 to 11-03-2015-05:04:07

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	DOS-Tool-SwitchbladG	dest-reset	2576
46.19.86.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
183.60.48.25	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

11-03-2015-04:04:07 to 11-03-2015-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.45.15.186	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
217.12.204.163	Ukraine	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
217.12.204.163	Ukraine	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

11-03-2015-04:04:07 to 11-03-2015-05:04:07

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	10
89.234.68.69	147.237.72.166	Ireland	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	10
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
66.249.84.69	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
5.39.222.253	147.237.76.38	Netherlands	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
188.138.9.51	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
119.123.112.210	147.237.72.14	China	dover.idf.il(old	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	147.237.77.19	Germany	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	147.237.0.19	Germany	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1

11-03-2015-04:04:07 to 11-03-2015-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	225
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
75.66.86.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
84.94.16.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
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
207.46.13.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.118.11.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop		drop	6
46.19.86.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.70.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.186.147.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
73.134.115.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.186.202.253	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.153.133.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.165.15.79	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
83.130.101.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.208.80.140	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
76.240.17.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
41.234.239.5	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

11-03-2015-04:04:07 to 11-03-2015-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.251	Block	2
212.179.155.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.140.141.3	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.46	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
79.180.146.88	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.146.88	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
172.56.40.93	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17047-h	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3493.jpg	Block	1
207.46.13.120	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.180.146.88	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
182.118.45.231	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	1
79.180.146.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
182.118.53.74	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/www.idf.il	Block	1
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/watercrafts.aspx	Block	1
89.234.68.69	Ireland	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 89.234.68.69 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
37.26.147.200	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
182.118.60.35	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
77.237.138.51	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
89.234.68.69	Ireland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

11-03-2015-04:04:07 to 11-03-2015-05:04:07