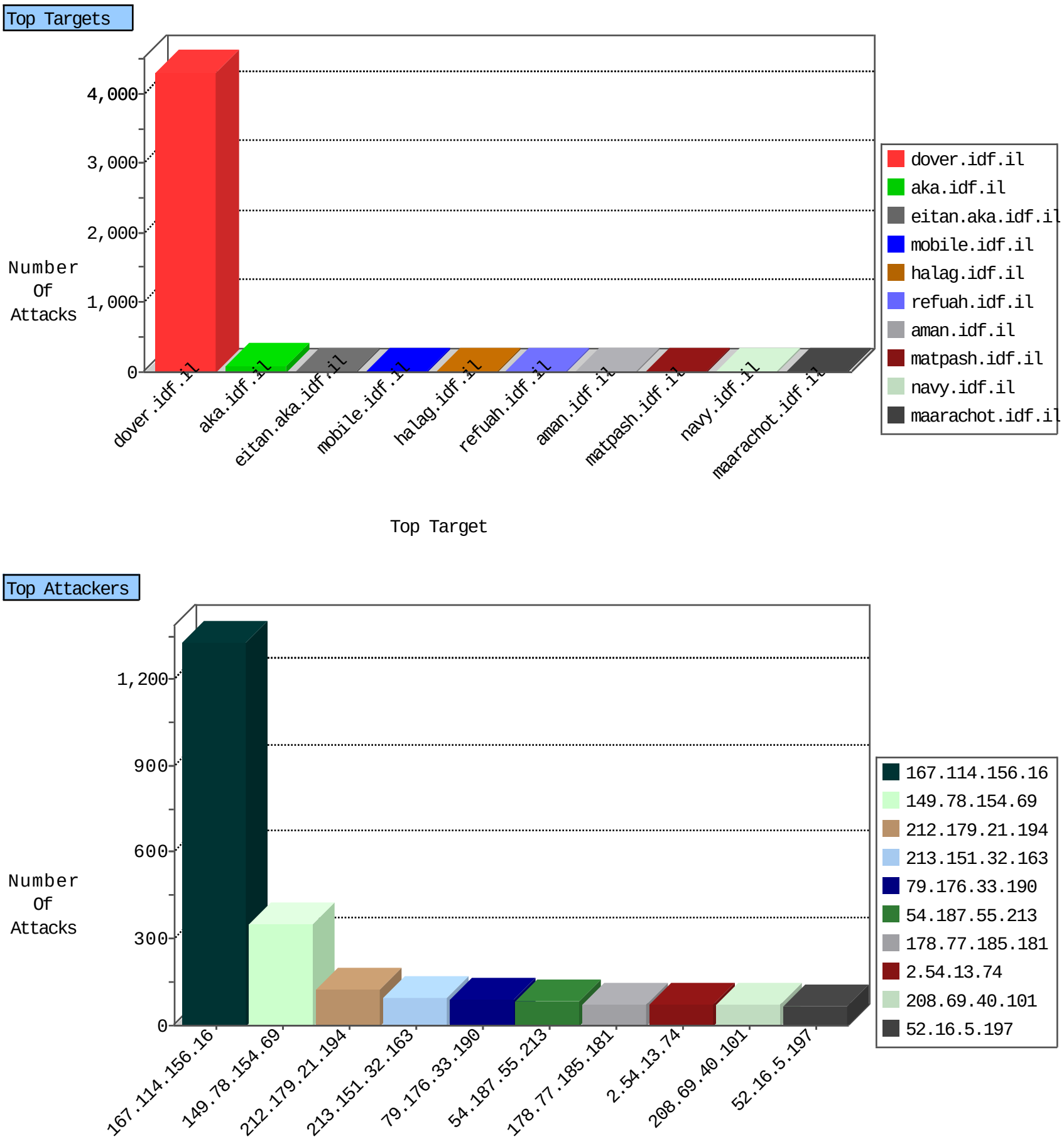
11-02-2015-06:04:02 to 11-02-2015-07:04:02

IDF Under Attack Daily Report



11-02-2015-06:04:02 to 11-02-2015-07:04:02

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	2402
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	477
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	87
174.236.96.48	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.34.117	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
107.107.58.116	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.13.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.139.12.92	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-02-2015-06:04:02 to 11-02-2015-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.113.143	France	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-02-2015-06:04:02 to 11-02-2015-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.113.143	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	11
62.210.113.143	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	11
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.34	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
198.12.96.232	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
120.24.225.16	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
120.24.225.16	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
120.24.225.16	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.113.143	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP printenv access	1
120.24.225.16	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
120.24.225.16	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
108.46.176.83	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.210.113.143	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP test.cgi access	1
62.210.113.143	147.237.77.216	France	dover.idf.il	GPL WEB_SERVER printenv access	1

11-02-2015-06:04:02 to 11-02-2015-07:04:02

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	351
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
213.151.32.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
79.176.33.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
2.54.13.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
178.77.185.181	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
168.235.200.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
24.147.46.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
38.80.238.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
46.116.200.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
192.0.81.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
46.120.163.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
151.80.34.225	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
81.218.140.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
76.94.180.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
62.210.113.143	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.52.171.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
104.153.147.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.19.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
107.14.54.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
107.14.54.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
107.77.70.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.34.90		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
150.135.210.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
76.122.195.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.178.112.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.178.197.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
173.252.88.246	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.65.189.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.34.90		147.237.76.42	refuah.idf.i	drop	First packet isn't SYN	drop	12

11-02-2015-06:04:02 to 11-02-2015-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
176.13.2.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/8/size220x0/17468.jpg	Block	2
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.88.98.13	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.74.98	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
2.52.171.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.155	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/login/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/110-he/patzar.aspx	Block	1
24.147.46.203	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
213.57.232.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.66	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	1
37.26.149.194	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.250.51.8	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	1
66.249.78.121	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on chinuch.aka.idf.il/404.htm	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.23.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17468.jpg	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1

11-02-2015-06:04:02 to 11-02-2015-07:04:02