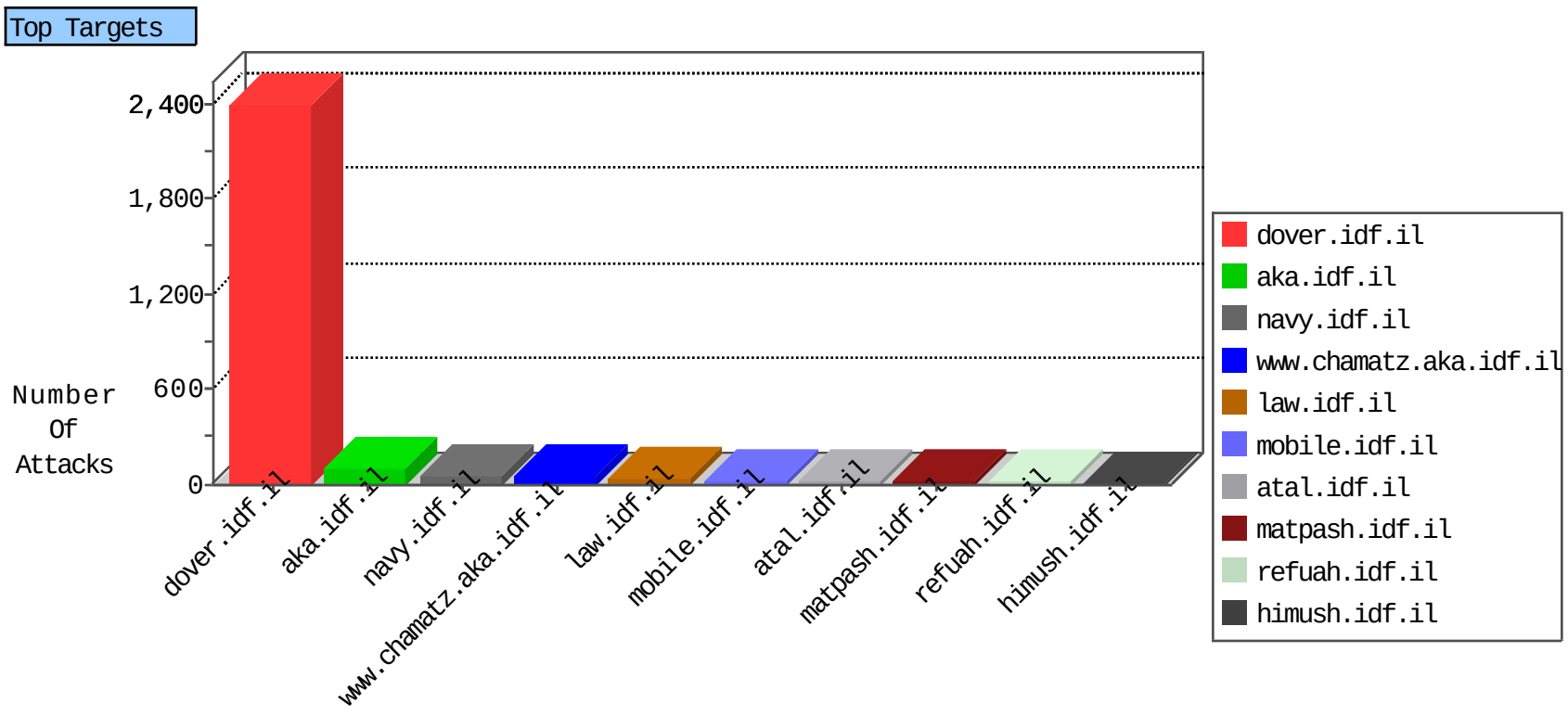
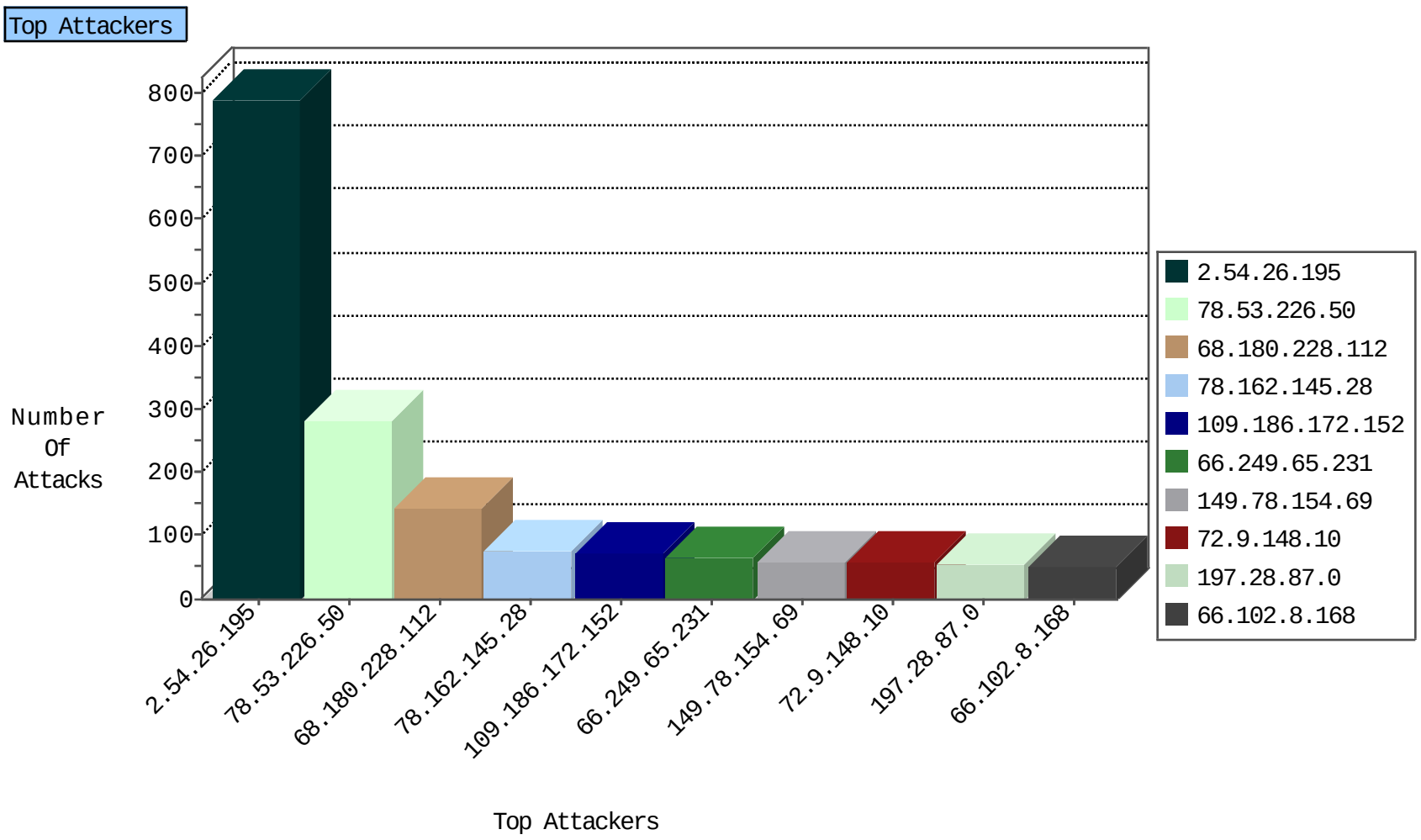
10-24-2015-02:04:09 to 10-24-2015-03:04:09

IDF Under Attack
Daily Report





10-24-2015-02:04:09 to 10-24-2015-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.211.16.251	Norway	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.54.46.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
64.233.172.162	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
94.102.49.122	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
141.212.121.219	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1

10-24-2015-02:04:09 to 10-24-2015-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

10-24-2015-02:04:09 to 10-24-2015-03:04:09

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	4
78.30.208.199	147.237.77.243	Russian Federation	mobile.idf.il	ET DOS SSL Bomb DoS Attempt	3
41.134.205.218	147.237.76.34	South Africa	yohalan.idf.il	ET SCAN Potential SSH Scan	1
158.69.207.180	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
158.69.207.180	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
103.232.35.93	147.237.72.217	Hong Kong	e.idf.il	ET SCAN NMAP -sS window 2048	1
90.151.211.40	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.253.96.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
41.134.205.218	147.237.76.42	South Africa	refuah.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
41.134.205.218	147.237.76.38	South Africa	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
179.124.44.98	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
41.134.205.218	147.237.76.31	South Africa	nakchal.idf.il	ET SCAN Potential SSH Scan	1
158.69.207.180	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
103.232.35.93	147.237.72.217	Hong Kong	e.idf.il	ET SCAN NMAP -sS window 3072	1
103.232.35.93	147.237.72.217	Hong Kong	e.idf.il	ET SCAN NMAP -f -sS	1
78.30.208.199	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
69.164.198.123	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.134.205.218	147.237.76.39	South Africa	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

10-24-2015-02:04:09 to 10-24-2015-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.26.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	790
78.53.226.50	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	273
78.162.145.28	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
109.186.172.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
197.28.87.0	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.156.187	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.37.161		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.233.229.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.84.166	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	17
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
88.238.81.103	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.64.100	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.112.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
64.237.233.176	Puerto Rico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.250.160.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
173.68.66.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
78.53.226.50	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
79.176.64.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.65.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
75.34.109.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
155.31.32.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.26.183.129	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

10-24-2015-02:04:09 to 10-24-2015-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/bagatz_sarbanim.stm_	Block	84
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
188.143.232.24	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	28
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	28
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	14
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/	Block	14
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19559-he/dover.aspx	Block	14
17.138.54.219	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	14
188.143.232.24	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1319-he/	Block	14
54.179.134.216	Singapore	147.237.76.30	himush.idf.il	Unauthorized URL Access to /	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	14
157.55.39.237	United States	147.237.77.216	dover.idf.il	Parameter Type Violation a in www.idf.il/	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	14
37.187.80.217	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	14
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	14
176.12.149.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news	Block	14
37.187.80.217	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/news/wp-admin/setup-config.php	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8867-he/refuah.aspx	Block	14
82.161.176.208	Netherlands	147.237.72.166	aka.idf.il	Unknown Parameter catId=43332 in www.aka.idf.il/kamlar/klali/default.asp	None	14
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
178.255.87.242	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/robots.txt	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	14
189.179.140.212	Mexico	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
82.161.176.208	Netherlands	147.237.72.166	aka.idf.il	Unknown Parameter catId=58564&docId=35721 in www.aka.idf.il/main/giyus/general.aspx	None	14

10-24-2015-02:04:09 to 10-24-2015-03:04:09