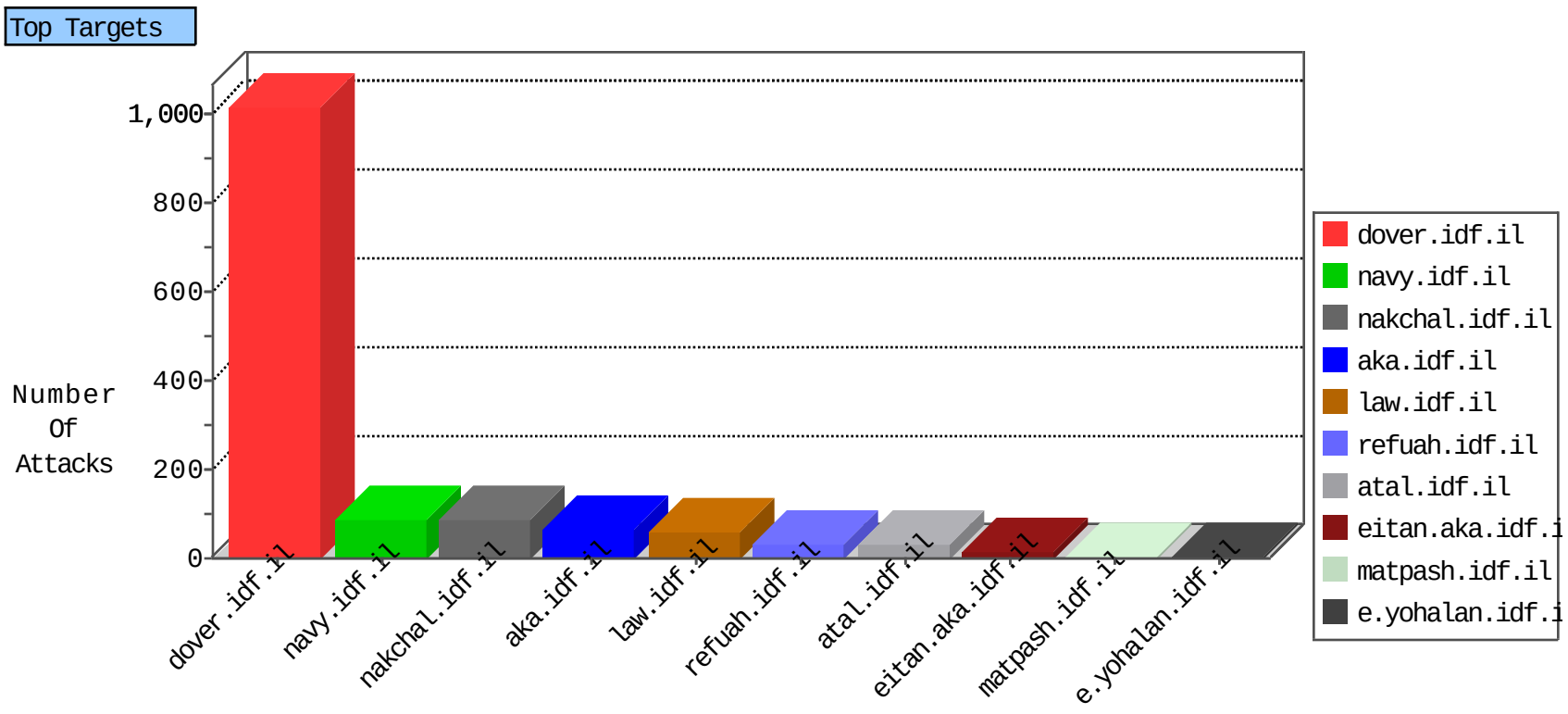
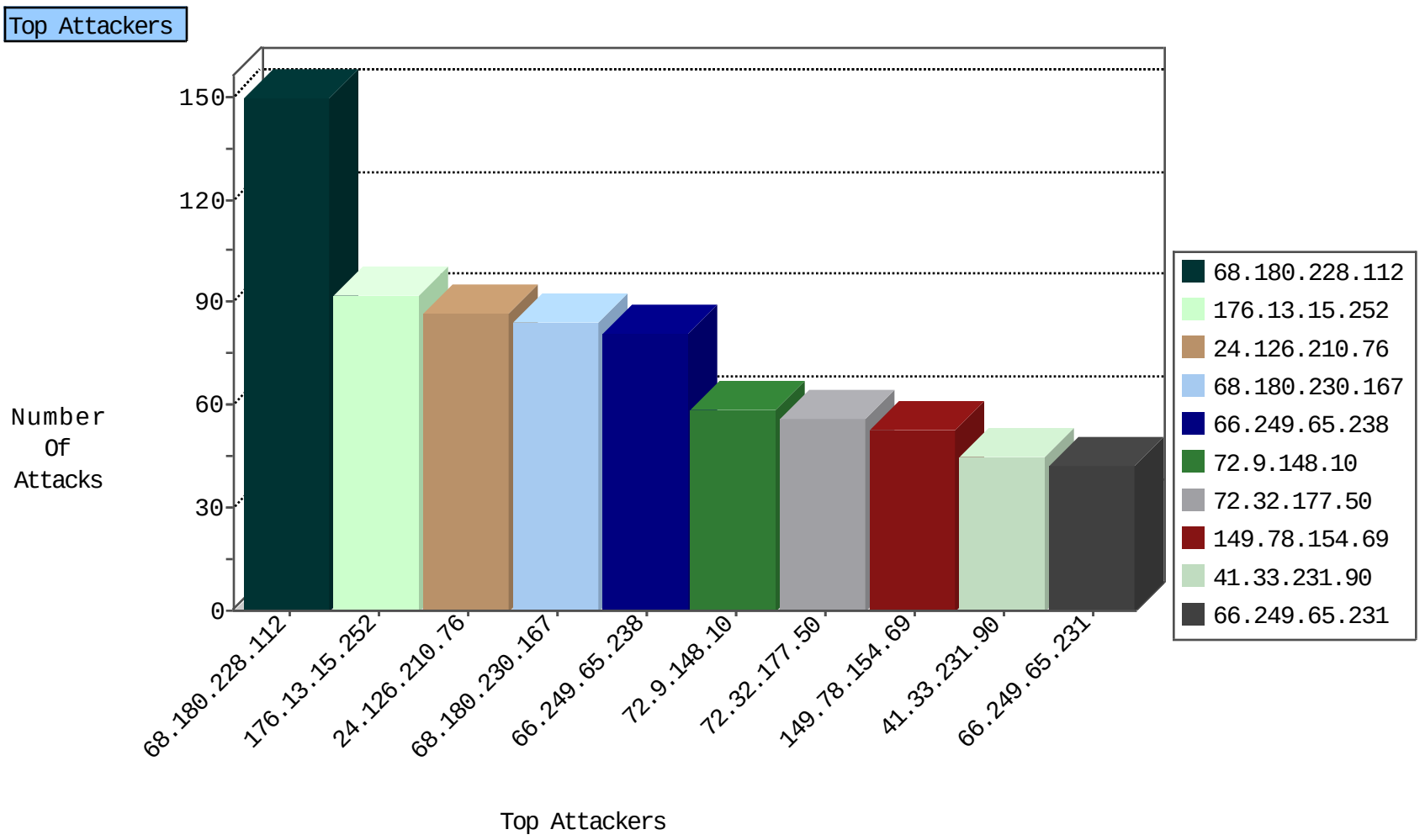
10-24-2015-04:04:05 to 10-24-2015-05:04:05

IDF Under Attack Daily Report





10-24-2015-04:04:05 to 10-24-2015-05:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	59
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	45
176.13.15.252	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
24.126.210.76	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.57.198.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
54.187.55.213	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
188.138.1.218	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-24-2015-04:04:05 to 10-24-2015-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-04:04:05 to 10-24-2015-05:04:05

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	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
142.54.163.74	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
142.54.163.74	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
69.164.207.141	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	147.237.0.33	Korea, Republic of	idf.il	ET SCAN NMAP -sS window 3072	1

10-24-2015-04:04:05 to 10-24-2015-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
24.126.210.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
176.13.15.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
209.141.43.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
206.21.125.108	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
78.53.226.50	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
98.113.28.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.121.107		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	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	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
64.235.56.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.127.29.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
186.13.3.1	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
38.111.147.88	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.40.60.21	Luxembourg	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
108.222.127.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
97.123.96.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.169.234.5	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.58.66.26	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
78.53.226.50	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.41	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.142.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.4.10.6	Germany	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-24-2015-04:04:05 to 10-24-2015-05:04:05

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/navy/html/historyfs.html	Block	84
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1110-he/nakhal.aspx	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
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
72.32.177.50	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	28
78.47.67.232	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	28
85.29.187.251	Kazakstan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	14
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
46.182.106.190	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	14
182.118.54.181	China	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../shared/clientscripts/jquery.plugins/slider.js	Block	14
72.32.177.50	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 72.32.177.50	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	14
91.191.151.99	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	14
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
91.191.151.99	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/test/wp-admin/setup-config.php	Block	14
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
188.165.15.200	France	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
72.32.177.50	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/blog/wp-admin/setup-config.php	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
141.212.122.160	United States	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to 147.237.76.200/	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.7	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
157.55.39.25	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14

10-24-2015-04:04:05 to 10-24-2015-05:04:05