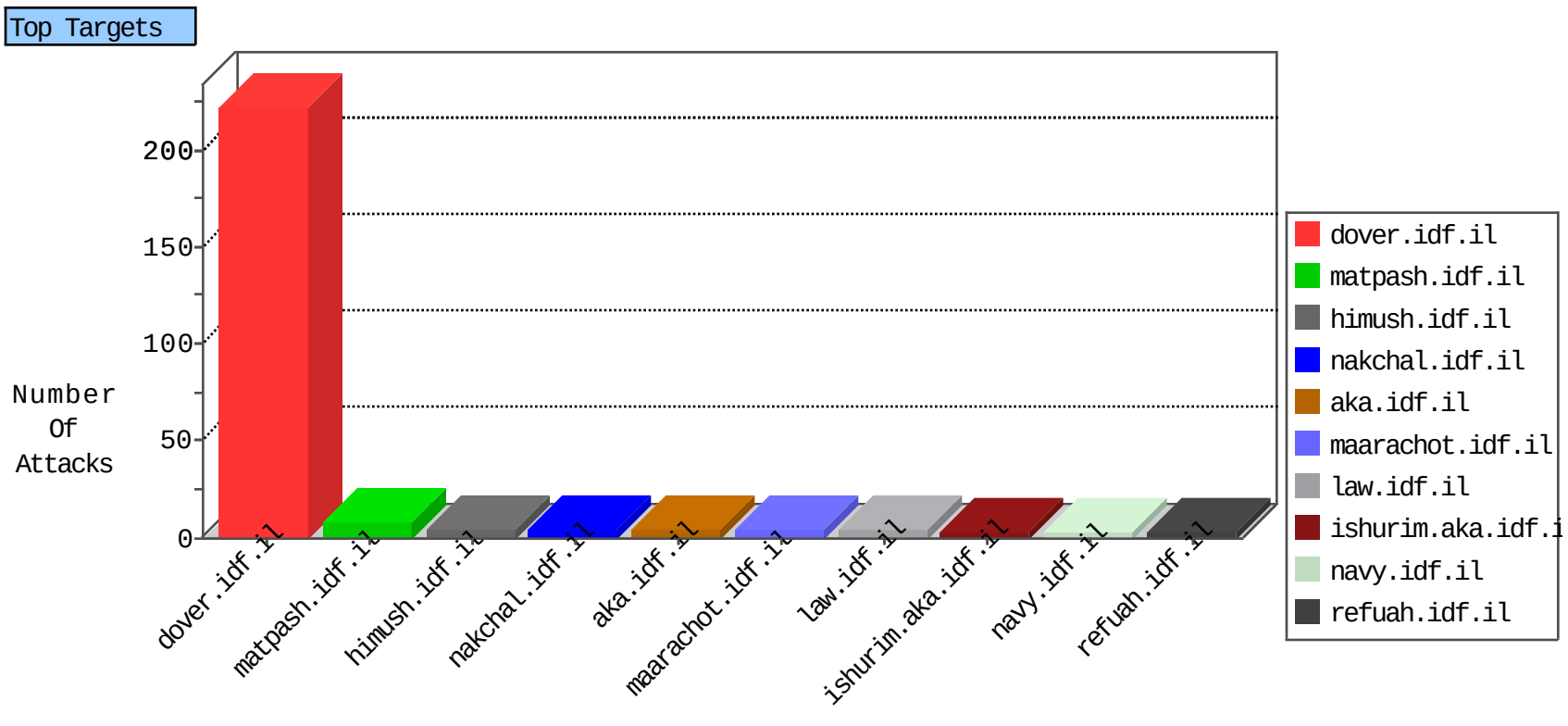
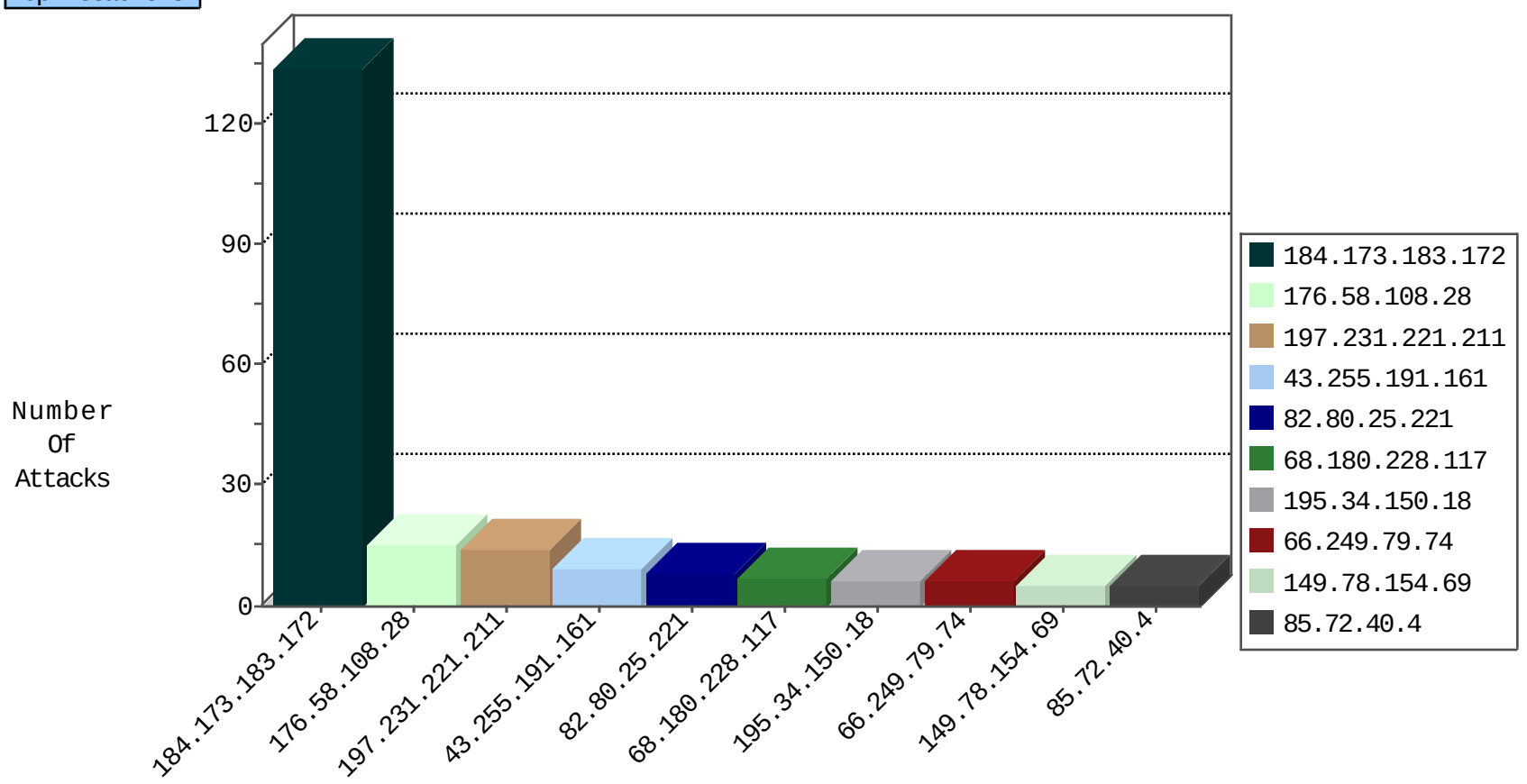
04-24-2015-04:03:09 to 04-24-2015-05:03:09

IDF Under Attack
04-24-2015-04:03:09

Top Targets



Top Attackers



04-24-2015-04:03:09 to 04-24-2015-05:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
68.180.228.117	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	818
220.181.108.154	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	396
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
212.224.87.250	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
23.95.84.186	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
23.95.84.186	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

04-24-2015-04:03:09 to 04-24-2015-05:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	134
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
187.95.34.3	Brazil	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-04:03:09 to 04-24-2015-05:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
54.147.46.79	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
168.187.246.41	Kuwait	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
118.71.243.177	Vietnam	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
82.166.91.43	Israel	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.236.90	France	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
210.51.56.174	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
168.187.246.41	Kuwait	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
168.187.246.41	Kuwait	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
118.71.243.177	Vietnam	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.236.90	France	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
210.51.56.174	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.76.197	e.himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1

04-24-2015-04:03:09 to 04-24-2015-05:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.216.30.246	Saudi Arabia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
174.129.237.157	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.65.5.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.13.100.116	Ireland	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
104.32.162.117		147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
123.125.71.12	China	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1
62.210.69.5	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
182.118.22.208	China	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1
192.99.170.80	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-24-2015-04:03:09 to 04-24-2015-05:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	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
104.171.124.74		147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
203.133.168.163	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.65.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	1
222.239.162.7	Korea, Republic of	147.237.77.216	dover.idf.il	Too Many Cookies in a Request - 105 cookies	Block	1
104.32.162.117		147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.65.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
157.55.39.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sachar	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
104.32.162.117		147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/640-en/text/javascript	Block	1
66.249.65.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
171.25.193.20	Sweden	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	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	1
66.249.65.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
104.171.124.74		147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.65.152	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	1
68.180.229.36	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.65.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1

04-24-2015-04:03:09 to 04-24-2015-05:03:09