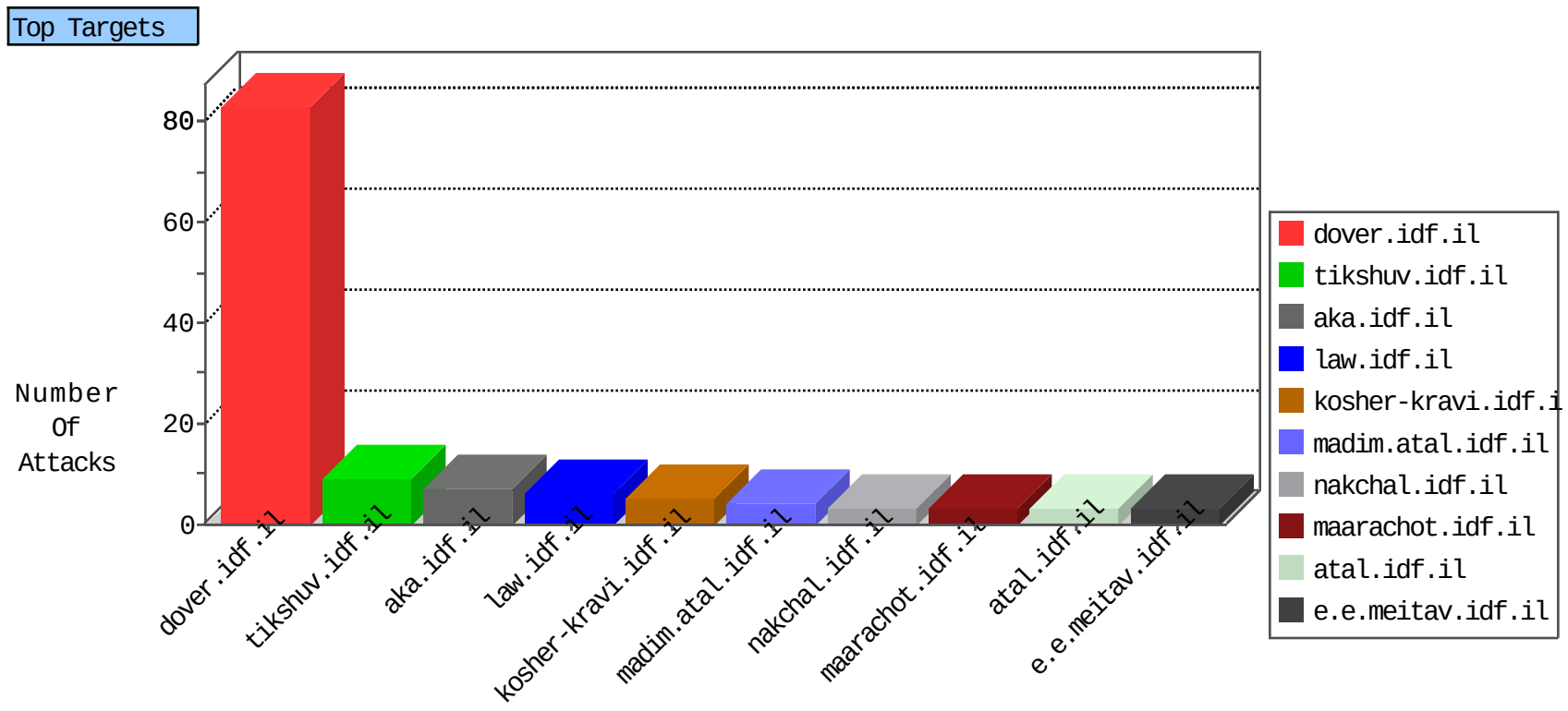
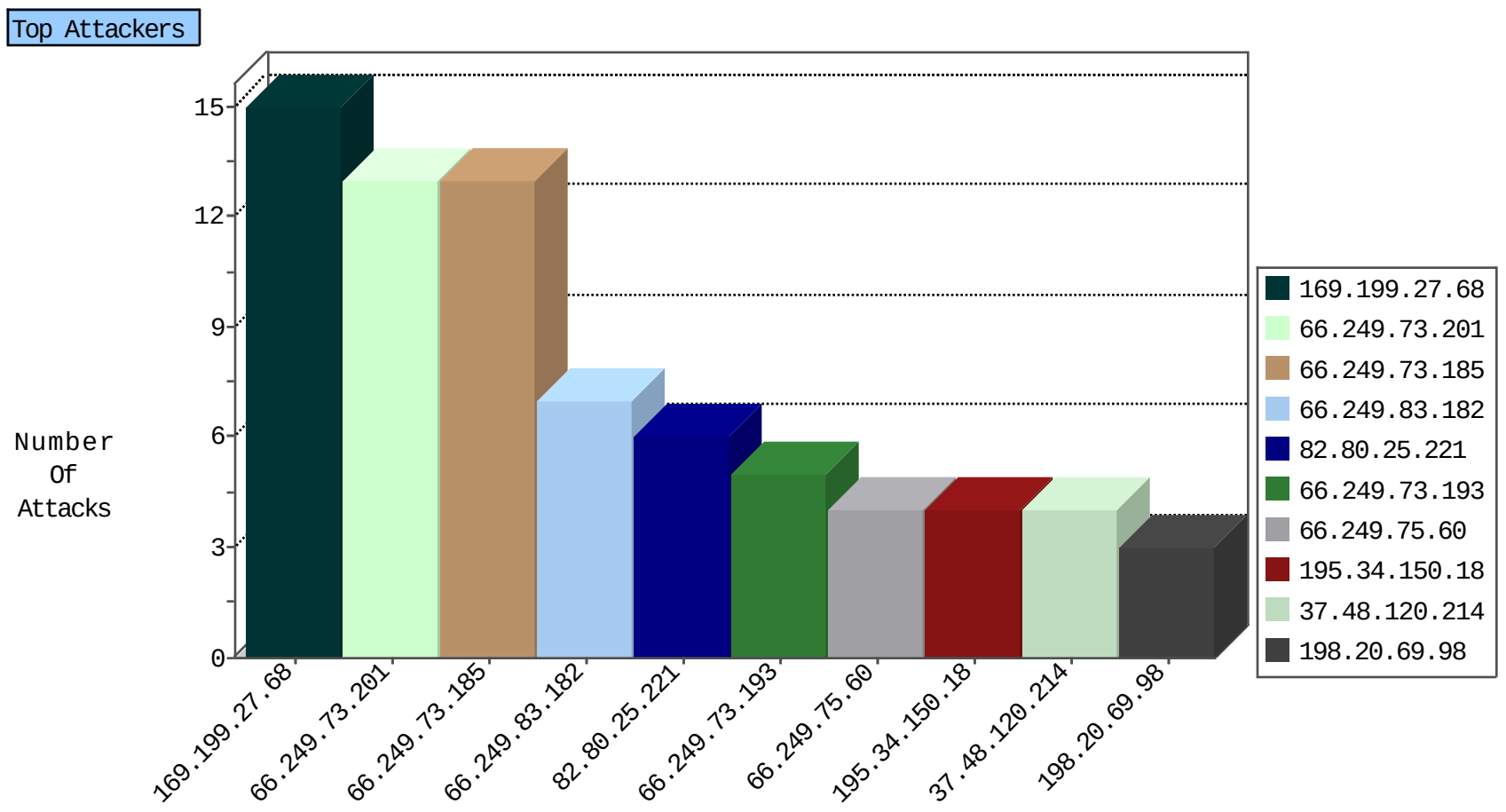
04-25-2015-03:03:01 to 04-25-2015-04:03:01

IDF Under Attack
04-25-2015-03:03:01

Top Targets



Top Attackers



04-25-2015-03:03:01 to 04-25-2015-04:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.93	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4356
66.249.83.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1437
112.118.235.106	Hong Kong	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-03:03:01 to 04-25-2015-04:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
74.102.70.91	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-03:03:01 to 04-25-2015-04:03:01

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	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
169.199.27.68	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
46.19.85.175	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
169.199.27.68	United States	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
169.199.27.68	United States	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
61.183.128.6	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.59	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.199.27.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
91.238.134.92	Poland	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.59	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.238.134.92	Poland	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2015-03:03:01 to 04-25-2015-04:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.83.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
104.173.218.214		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.142.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
108.5.117.217	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.83.188	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.165.15.13	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.145.210.21	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.136.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
213.57.135.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
220.255.1.135	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.242.135.175	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.128.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.134.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.82.78.119	Portugal	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
104.32.162.117		147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-25-2015-03:03:01 to 04-25-2015-04:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	13
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	11
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	5
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
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.asp	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.75.80	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.75.80	Block	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
169.199.27.68	United States	147.237.0.34	tikshuv.idf.il	Access to: /cgi-bin/php	Block	1
192.34.59.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/undefined	Block	1
169.199.27.68	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Malformed URL from 169.199.27.68	Block	1
66.249.75.80	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
66.249.69.122	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.199.27.68	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim	Block	1
203.133.169.214	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
169.199.27.68	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/cgi-bin/php	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
169.199.27.68	United States	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.249.75.23	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2003/may/18.stm	Block	1
169.199.27.68	United States	147.237.0.19	madim.atal.idf.il	Malformed URL http/1.1	Block	1
67.70.143.137	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.120.153.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.51	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58623&docid=77022	Block	1
169.199.27.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/cgi-bin/php	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0202-6.stm	Block	1

04-25-2015-03:03:01 to 04-25-2015-04:03:01