

Canadian Centre for Child Protection has seen a variety of responses to the notices issued and the removal of material through Project Arachnid. In some cases notices from Project Arachnid have been whitelisted by certain ESPs and material is removed within a matter of minutes of a notice being issued. Of the material hosted on the public Internet that Project Arachnid detects and issues notices on, 15% is removed within 1 day and 50% of the material is removed within 4 days of a notice being issued. The least responsive ESPs, which make up approximately 10% of the notices, take on average almost 2 weeks to remove material.

70. The Canadian Centre for Child Protection also runs into roadblocks getting CSAIO removed from the dark web as well as from so-called “bulletproof” hosting services which are services that are provided by some domain hosting or web hosting companies. These companies provide considerable leniency in the kinds of material they allow their customer to upload and make available, which can include “child pornography”.

71. Since the beginning of 2019, Project Arachnid had detected more than 5,500 dark web URLs as hosting CSAIO without any recourse to send notices for the removal of the material. Project Arachnid also detected more than 10,000 URLs for images of CSAIO on three domains administered and hosted by a bulletproof hoster in the public domain. Neither the hosting provider nor the sites administrator have responded and much of the material continues to remain online.

72. Project Arachnid issues notices on CSAIO related to prepubescent children as well as identified pubescent/ post-pubescent children. While the material in both of these groups is illegal, the typical methods of distribution and locations where the CSAIO is found differs between prepubescent victims and pubescent/post-pubescent victims.

73. Project Arachnid detects a large volume of CSAIO related to prepubescent victims that is made available on dark web forums, but actually sits on open web sources in encrypted archives. These encrypted archives cannot be detected by industry using real-time scanning techniques. Offenders post the