С начала марта 2024 года специалисты F.A.C.C.T.Threat Intelligence выявили новый вредоносный загрузчик PhantomDL (PhantomGoDownloader), ранее неизвестный им. После анализа обнаруженных образцов они обнаружили связи с группой PhantomCore и приписали PhantomDL к этой же группировке. В новом блоге компании приведены подробности об этом.

Группа PhantomCore, действующая с начала 2024 года, была раскрыта и описана в отчёте исследователей F.A.C.C.T. Она направлена против российских организаций. Первоначальный метод распространения загрузчика неизвестен, но группа использовала фишинговые письма с вредоносными архивами для заражения компьютеров.

В конце марта специалисты F.A.C.C.T.Threat Intelligence обнаружили исполняемый файл на VirusTotal, содержащий легитимный PDF-файл и вредоносный исполняемый файл с загрузчиком PhantomDL. Архив с этими файлами использовал уязвимость WinRAR — CVE-2023-38831. Если версия WinRAR меньше 6.23, то запускается вредоносный файл, а при версии 6.23 и выше отображается легитимный PDF.

Злоумышленники используют качественные документы-приманки, направленные на российские предприятия, а также качественные загрузчики, такие как PhantomDL, который продемонстрировал усовершенствования по сравнению с предыдущими версиями.