В первую очередь закидываю файл в DIE и вижу, что очень большая энтропия у секции text, предполагаю, что файл упакован. Закидываю файл в IDA и вижу, что у него нет импортов и всего 4 функции, это точно указывает на то, что файл упакован. Перехожу в строки и вижу: «This file is packed with the UPX executable packer», «upx UPX 4.10 Copyright (C) 1996-2023 the UPX Team. All Rights Reserved», это значит, что файл упакован UPX. Благо UPX предоставляет возможность как упаковки, так и распаковки.

Распакованный файл открываю в IDA и вижу, что программа написана на языке C++, открываю плагин «Class Informer», который показывает классы и таблицы виртуальных функций, восстановленные из RTTI, но, к сожалению, вижу, что он поддерживает только MSVC.

При старте программа выводит приветственное сообщение, получает имя пользователя из переменной окружения и формирует строку, которая содержит путь «/Users/ИмяПользователя/Documents». Потом идет поиск документов с расширениями .txt, .docx, .doc, .pdf. Создается директория «/var/tmp/todo\_collected» и в нее копируются найденные документы. После чего они архивируются в архив с названием «archive.tar.gz» и отправляются с помощью утилиты curl на «<http://localhost:1234>».

Программа получает имя пользователя через переменную окружения, техника T1033(System Owner/User Discovery). Идет поиск и сбор документов, техника T1083(File and Directory Discovery) и T1005(Data from Local System). Происходит архивация найденных документов, техника T1560(Archive Collected Data). Происходит эксфильтрация архива, техника T1020(Automated Exfiltration).

Можно отслеживать запуск новых процессов, вызовы API, выполнение команд с аргументами. Например, можно отслеживать нетипичные попытки доступа к файлам с расширениями .pfd, .docx и т.д., отслеживать недавно созданные сетевые соединения, проверять являются ли узлы аномальными, отслеживать выполнения команд для сжатия. Сделать систему, которая маркирует подозрительные действия и при определенном пороге маркеров или при совпадении паттерна маркеров помечает конченый узел как зараженный. При этом создается свой паттерн маркеров для разного ВПО.