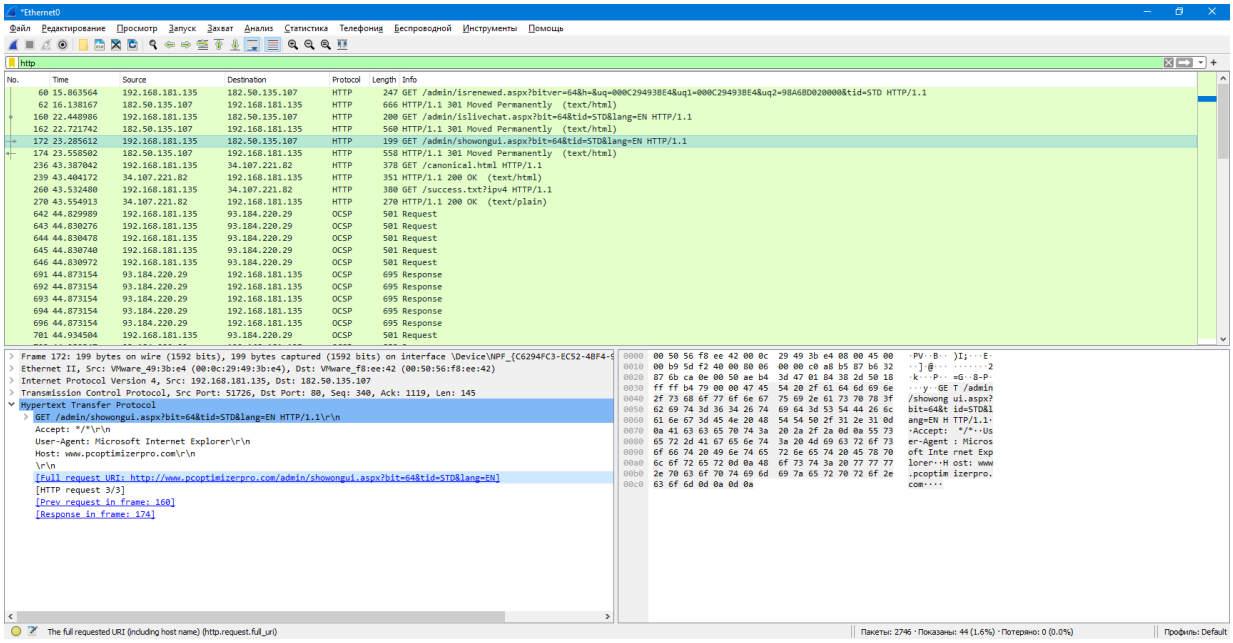
Статический анализ

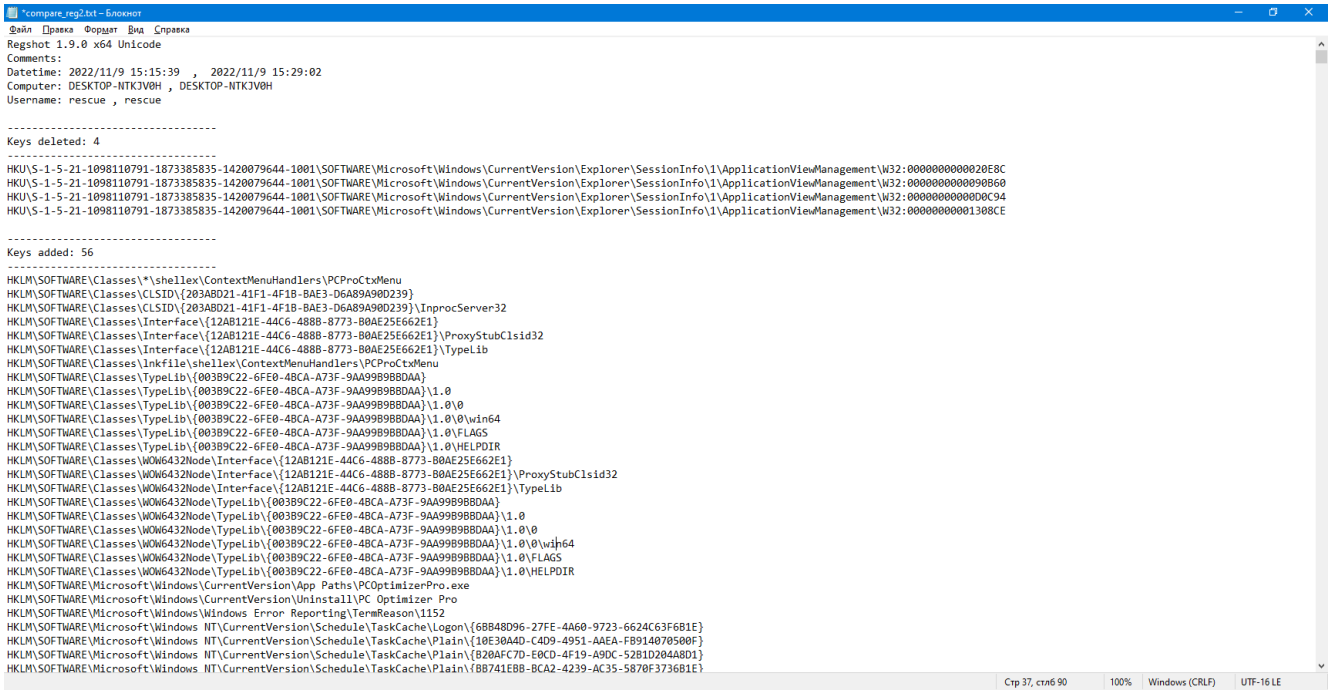
Задание представлено в виде файла «PCOptimizerProInstaller.exe». Первичный осмотр файла в IDA Pro не даль особых результатов, кроме вывода о том, что файл является инсталлятором.

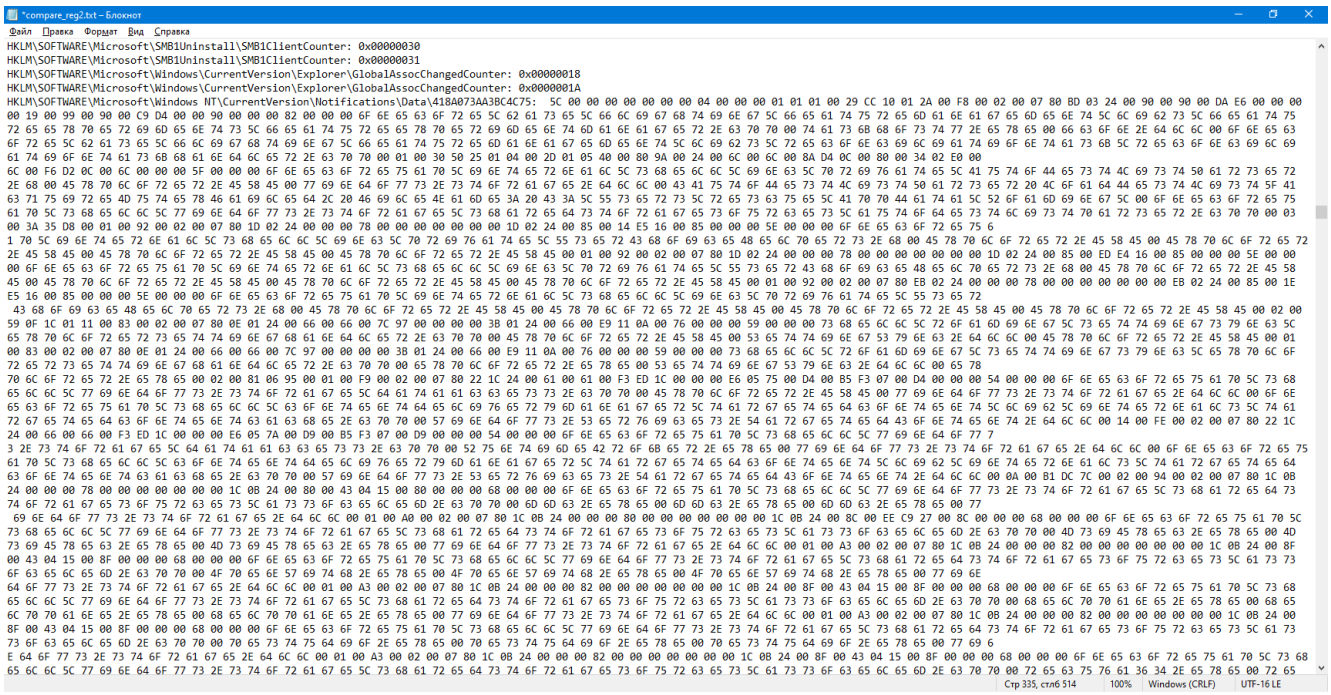
Динамический анализ

Вооружившись снимками реестра и автозагруки и запустив procmon с wireshark, начинается установка программы. После запуска устанавливается TCP соединение и в wireshark можно увидеть 3 HTTP запроса в момент запуска hxxp[:]//www.pcoptimizerpro.com/admin/*.

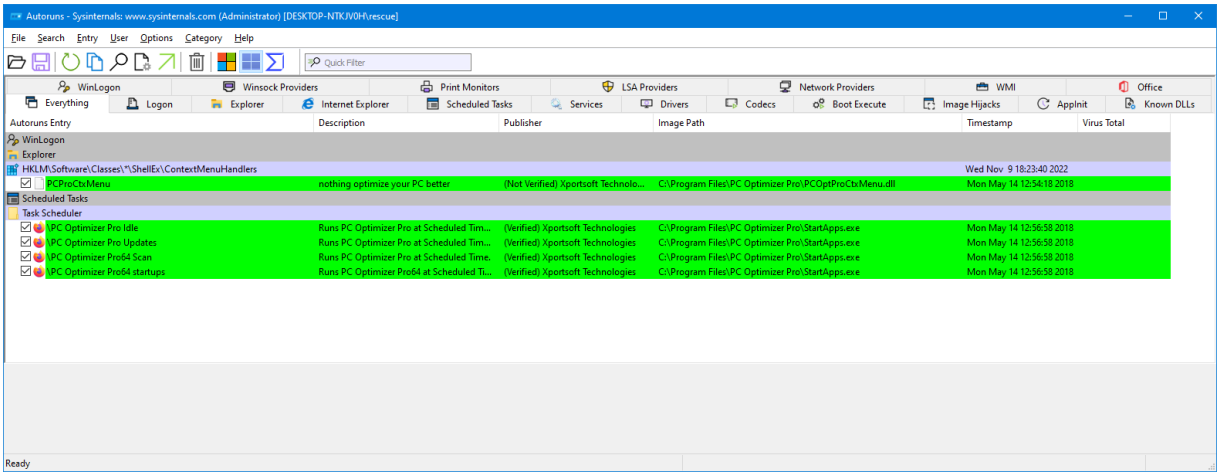


В реестр добавились записи о новых задачах, добавленном элементе в контестное меню, служебная информация для установленного приложения и WNF.

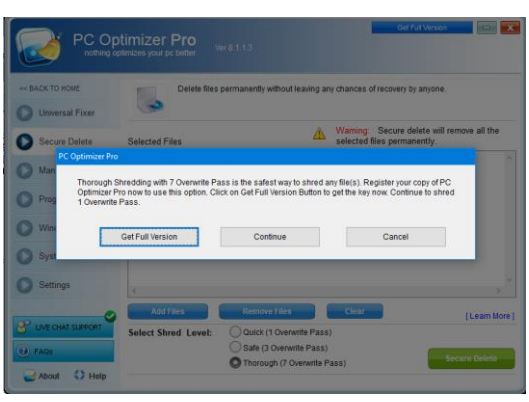




Также можно ознакомиться с сравнением состояний в autoruns. Видно, что создано 4 различных задачи для различных состояний системы. Они используют PC Optimizer Pro\StartApps.exe с различными аргументами при активации тригера задачи



Подозрительных операции во время простоя не было замечено, как и сетевого взаимодействия с доменом разрабатывающей компании. Функционал программы содержит опции: сканирования, перетирания данных, менеджер деинсталляции и автозапуска, плитки запускающие стандартные средства администрирования Windows. При попытках воспользоваться уникальным функционалом программы пользователю предлагается приобрести лицензию.



Вывод

Взглянув на файл «StartApps.exe» в IDA Pro и воспользовавшись дебаггером x64dbg, чтоб отладить процесс самого оптимайзера, не было выявлено зловредного поведения. ПО является сканером-оптимайзером системы, относится в категории нежелательной к использованию. Следовательно, PCOptimizerPro является программой, которая вынуждает пользователей оплатить лицензию, чтобы пользоваться функционалом.