File Name: e-Archive Dekont.exe

MD5 Hash: 7a0093c743fc33a5e111f2fec269f79b

SHA256
Hash: 722ef401e5cbb067c5c33faa402774d3c75ef08e0c8cc4d7e66a9cfa53684088

Поведенческий\Динамический анализ

Используемые инструменты:

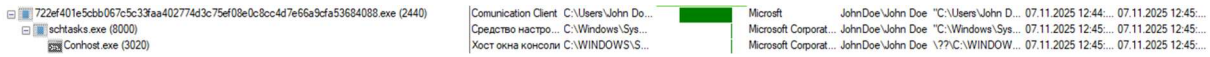
- Wireshark & Fiddler

- Procmon

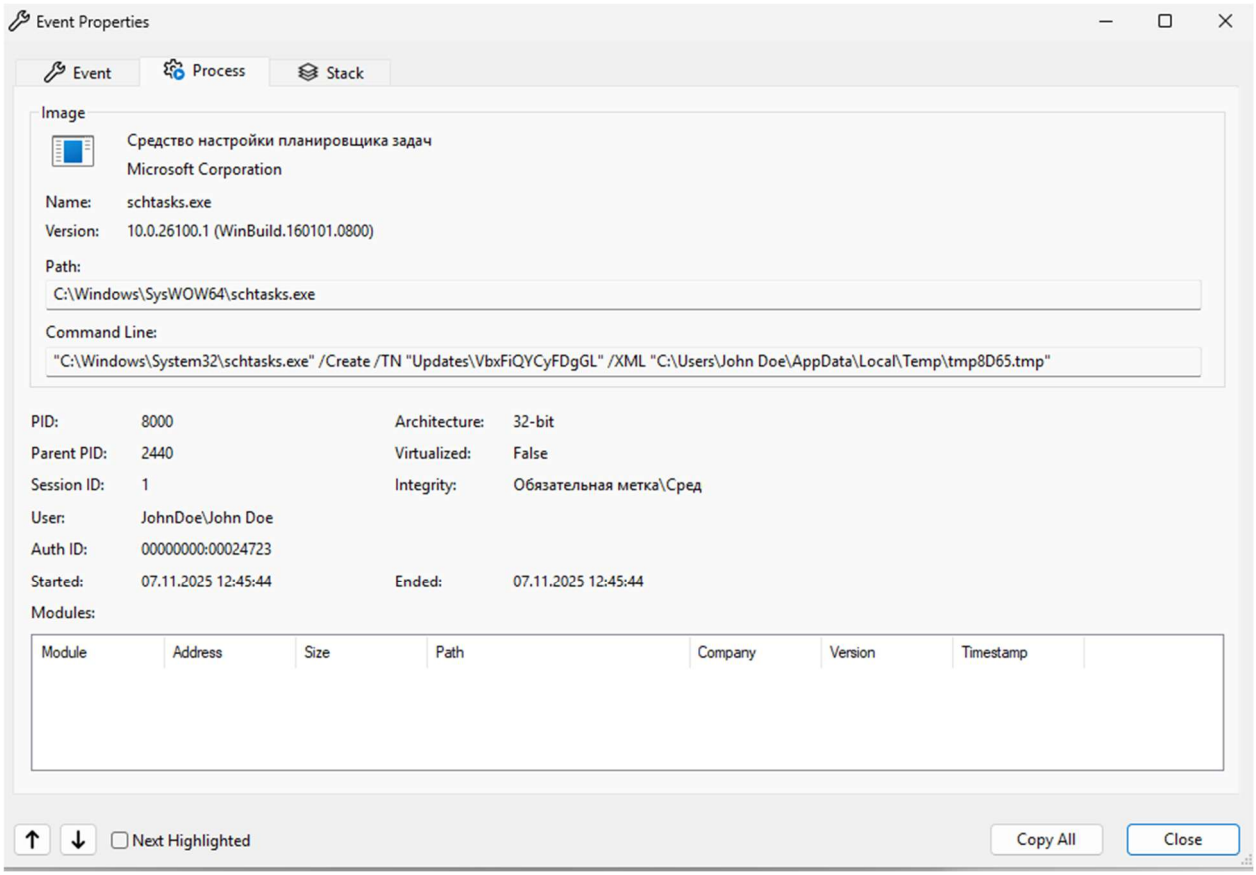
- Process Hacker 2

Контролируемый запуск и поведение:

При запуске создает Родительский процесс и два дочерних (вложенных последовательно).

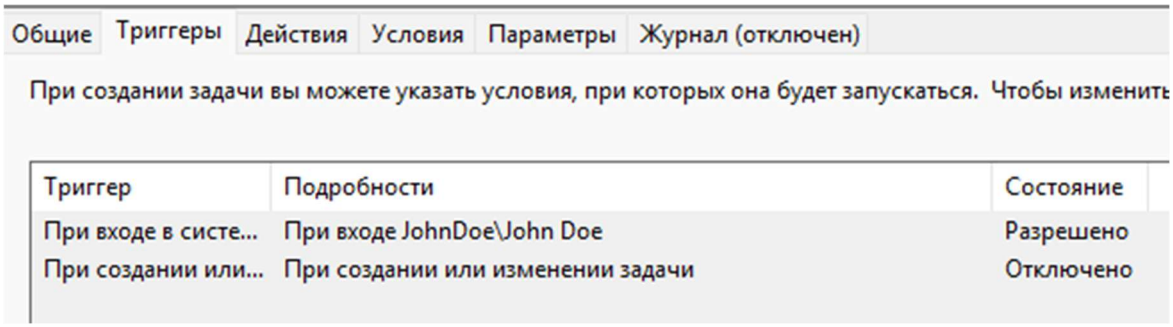


При этом была создана задача в планировщике:

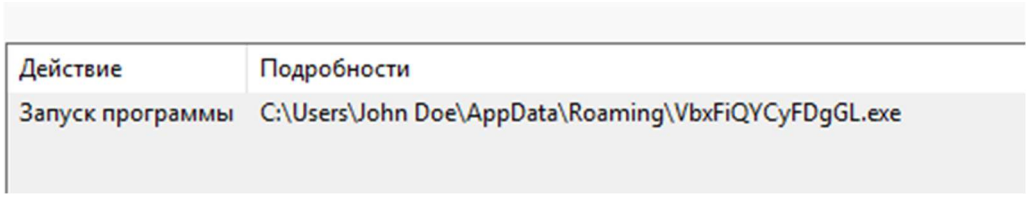


Смотрим в планировщике задачу:

1) Срабатывает при входе в систему

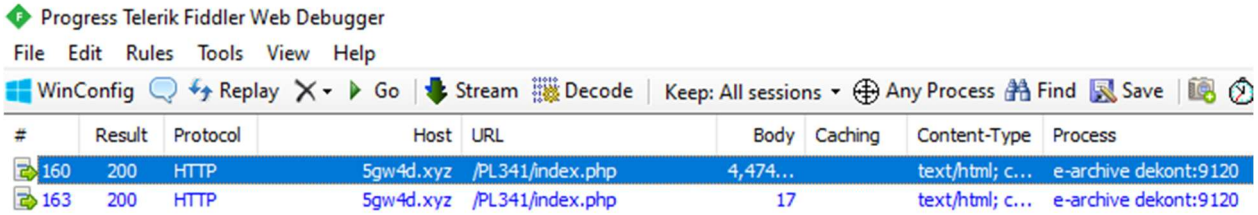


2) Запускает программу



По хешу она такая же, что и запускаемый файл – малварь скопировал туда сам себя.

Сетевая активность:



Изменение регистров:

Наследил в HKLM\Software\WOW6432Node\Microsoft\Windows\CurrrentVersion\Uninstall

Файловая активность:

Стилит данные из ЛогинДата браузеров

Заключение:

Малварь-стилер, копирует сам себя в АппДата, ставит процесс в планировщике на запуск при входе в систему, при этом стилит данные из браузеров. Прогнозирую кражу логинов-паролей и других чувствительных данных (номера карт и т.п.). Данные по идее отправляются на адрес в разделе «Сетевая активность». Изучить внутрянку программы не удалось – декомпилятор Ghidra не

справился с декомпиляцией ветки main. Другой информации, как то: строки, данные, артефактный экспорт\импорт вытащить не удалось.

На будущее: возможно, стоит провести контролируемый запуск под отладкой, чтобы увидеть в деталях, хотя зачем?