

**File Name:** e-Archive Dekont.exe

**MD5 Hash:** 7a0093c743fc33a5e111f2fec269f79b

**SHA256**

**Hash:** 722ef401e5ccb067c5c33faa402774d3c75ef08e0c8cc4d7e66a9cfa53684088

## Поведенческий\Динамический анализ

### Используемые инструменты:

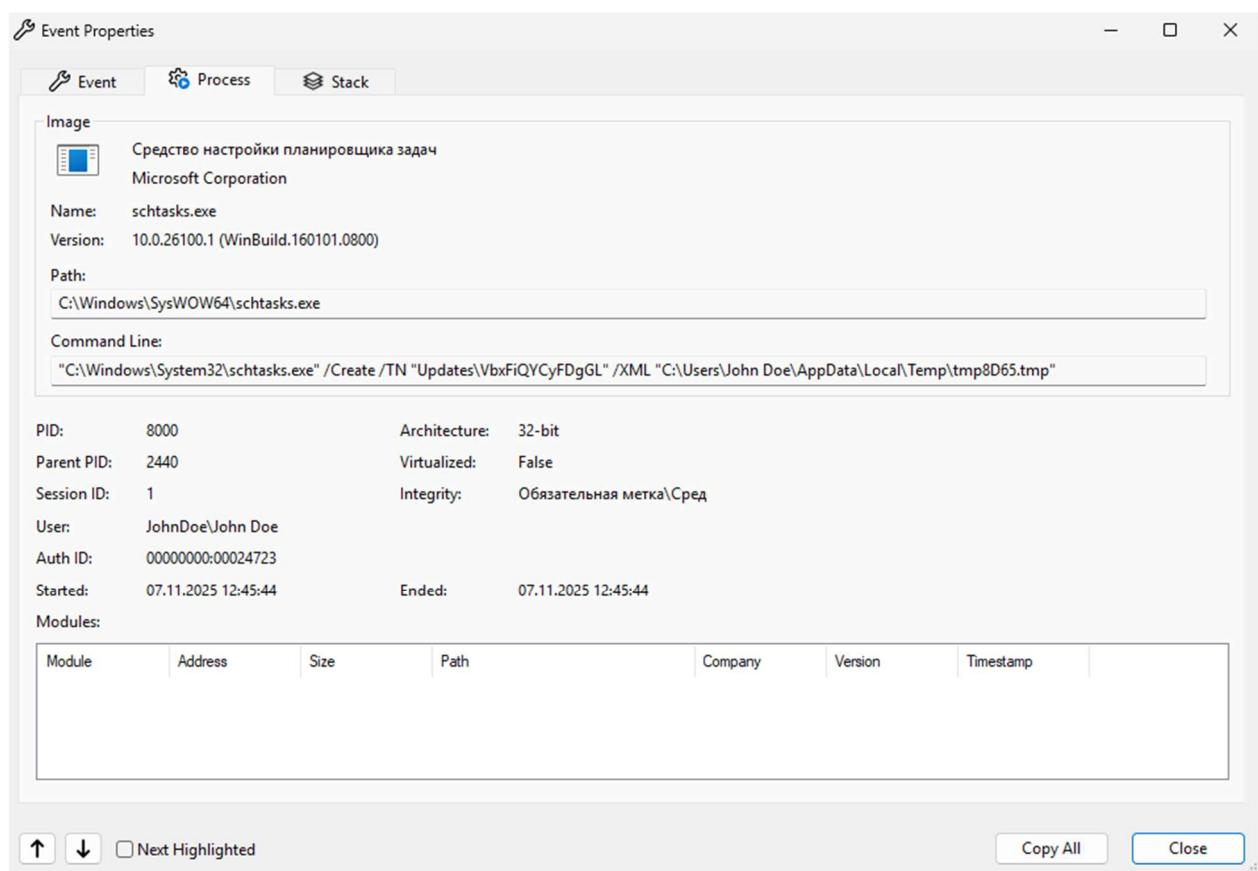
- Wireshark & Fiddler
- Procmon
- Process Hacker 2

### Контролируемый запуск и поведение:

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



При этом была создана задача в планировщике:



**Event Properties**

**Event** **Process** **Stack**

**Image**  
Средство настройки планировщика задач  
Microsoft Corporation

**Name:** schtasks.exe  
**Version:** 10.0.26100.1 (WinBuild.160101.0800)  
**Path:** C:\Windows\SysWOW64\schtasks.exe

**Command Line:**  
"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VbxFiQYCyFDgGL" /XML "C:\Users\John Doe\AppData\Local\Temp\tmp8D65.tmp"

**PID:** 8000      **Architecture:** 32-bit  
**Parent PID:** 2440      **Virtualized:** False  
**Session ID:** 1      **Integrity:** Обязательная метка\Сред  
**User:** JohnDoe\John Doe  
**Auth ID:** 00000000:00024723  
**Started:** 07.11.2025 12:45:44      **Ended:** 07.11.2025 12:45:44

**Modules:**

Module	Address	Size	Path	Company	Version	Timestamp

**Next Highlighted** **Copy All** **Close**

Смотрим в планировщике задачу:

- 1) Срабатывает при входе в систему

The screenshot shows the Windows Task Scheduler interface. At the top, there are tabs: Общие (General), Триггеры (Triggers), Действия (Actions), Условия (Conditions), Параметры (Parameters), and Журнал (отключен) (Log (disabled)). The Триггеры tab is selected. A message below the tabs says: 'При создании задачи вы можете указать условия, при которых она будет запускаться. Чтобы изменить' (When creating a task, you can specify conditions under which it will run. To change). Below this, there are two trigger entries:

Триггер	Подробности	Состояние
При входе в систему...	При входе JohnDoe\John Doe	Разрешено
При создании или...	При создании или изменении задачи	Отключено

- 2) Запускает программу

The screenshot shows the Windows Task Scheduler interface. The Actions tab is selected. It displays a single action entry:

Действие	Подробности
Запуск программы	C:\Users\John Doe\AppData\Roaming\VbxFiQYCyFDgGL.exe

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

#### Сетевая активность:

The screenshot shows the Fiddler network debugger interface. The main window displays two captured sessions:

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
160	200	HTTP	5gw4d.xyz	/PL341/index.php	4,474...		text/html; c...	e-archive dekont:9120
163	200	HTTP	5gw4d.xyz	/PL341/index.php	17		text/html; c...	e-archive dekont:9120

#### Изменение регистров:

Наследил в

HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\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 внутренку 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?*