

File Name: e-Archive Dekont.exe

MD5 Hash: 7a0093c743fc33a5e111f2fec269f79b

SHA256

Hash: 722ef401e5cbb067c5c33faa402774d3c75ef08e0c8cc4d7e66a9cfa53684088

Поведенческий\Динамический анализ

Используемые инструменты:

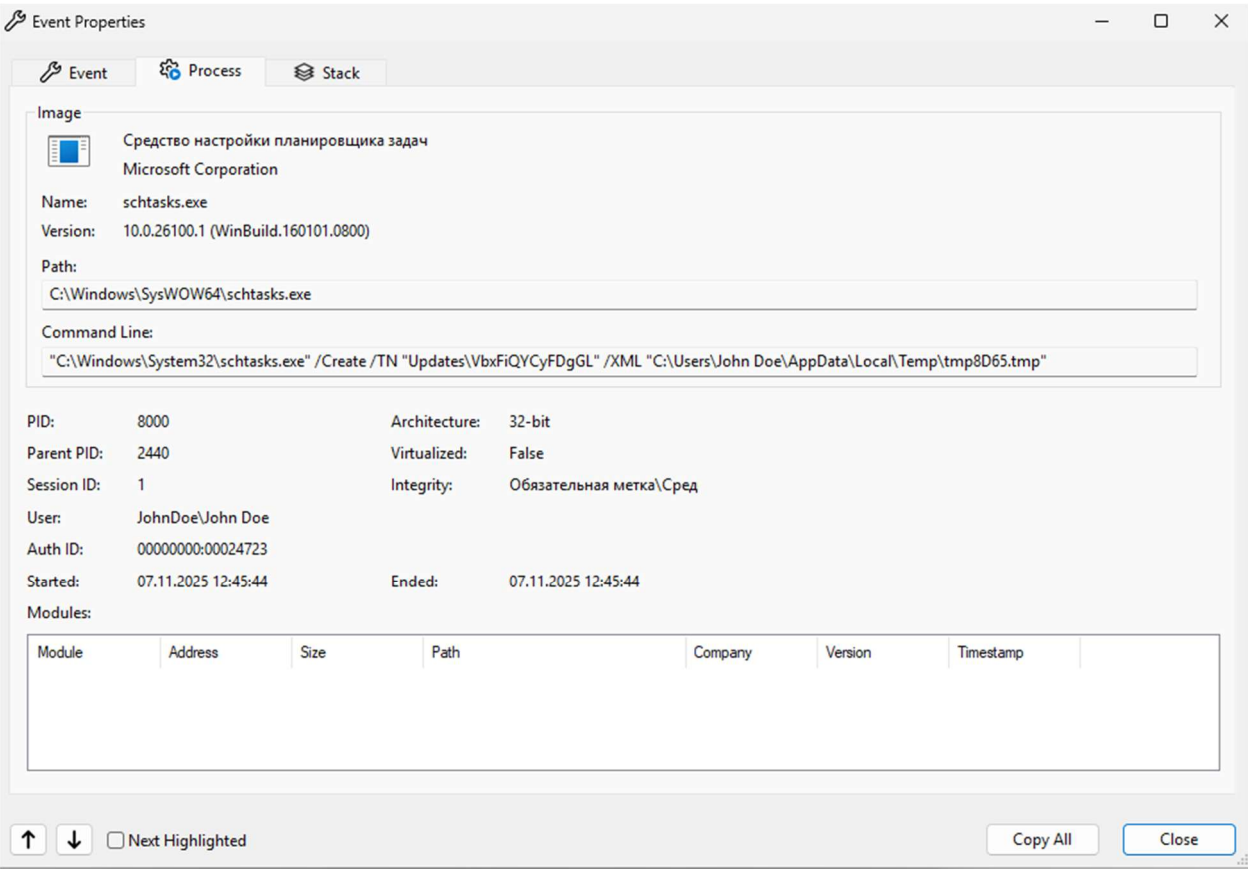
- Wireshark & Fiddler
- Procmon
- Process Hacker 2

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

Общие	Триггеры	Действия	Условия	Параметры	Журнал (отключен)
При создании задачи вы можете указать условия, при которых она будет запускаться. Чтобы изменить					
Триггер	Подробности	Состояние			
При входе в систе...	При входе JohnDoe\John Doe	Разрешено			
При создании или...	При создании или изменении задачи	Отключено			

- 2) Запускает программу

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:

Progress Telerik Fiddler Web Debugger										
File Edit Rules Tools View Help										
WinConfig Replay X Go Stream Decode Keep: All sessions Any Process Find Save										
#	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 AppData, ставит процесс в планировщике на запуск при входе в систему, при этом стилист 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?