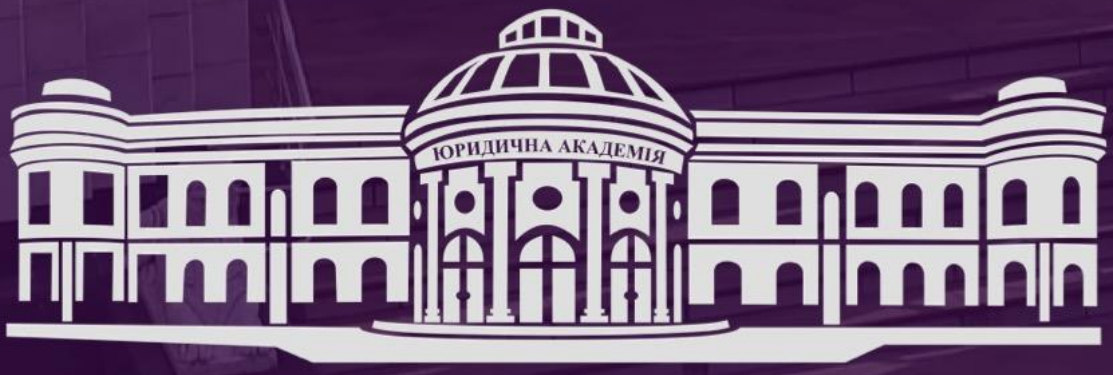
Національний університет «Одеська юридична академія»
Факультет прокуратури та слідства (кримінальної юстиції)
Кафедра криміналістики, судових експертиз та поліграфології

Національний центр судових експертиз при
Міністерстві юстиції Республіки Молдова
Одеський науково-дослідний інститут судових
експертиз Міністерства юстиції України

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: МІЖНАРОДНИЙ ДОСВІД ТА НАЦІОНАЛЬНА ПРАКТИКА»

27 листопада 2025 року, місто Одеса



EXPERT SUPPORT IN THE INVESTIGATION OF ORGANIZED CRIME: INTERNATIONAL EXPERIENCE AND NATIONAL PRACTICE

Proceedings of the International Scientific and Practical Conference

27 November 2025

Odesa
2025

УДК 340.6:343.9.022 (062)

Рекомендовано до друку рішенням кафедри криміналістики, судових експертиз та поліграфології НУ«ОЮА» (протокол № 9 від 24 листопада 2025 року)
Рекомендовано до друку рішенням Вченої ради ОНДІСЕ (протокол №9 від 1 грудня 2025 року)

Експертне забезпечення розслідування організованої злочинності: міжнародний досвід та національна практика: збірник матеріалів міжнар. наук.-практ. конф. м. Одеса, 27 листоп. 2025 р. / [орг. комітет: С. Ківалов, М. Аракелян, О. Катарага, Д. Кішко, Д. Колодін, А. Колодіна, Л. Аркуша та ін.]; Нац. ун-т Одеськ. юрид. акад. кафедра криміналістики, суд. експертиз та поліграф.; Нац. центр суд. експерт. при Міністер. юстиц. Респуб. Молдова; Одеськ. Наук.-дослідн. ін-т суд. експер. Міністер. юстиції України. Одеса: НУ «ОЮА», 2025. 450 с.

У збірнику викладено матеріали Міжнародної науково-практичної конференції «Експертне забезпечення розслідування організованої злочинності: міжнародний досвід та національна практика», в якій взяло участь понад 100 науковців і практиків з України та інших держав Європи. Представлено актуальні дослідження обговорень таких наукових і практичних проблем, як: експертне забезпечення протидії окремим видам організованої злочинності; використання спеціальних знань та експертне забезпечення розслідування організованої злочинності в умовах збройного конфлікту; міжнародна співпраця у сфері експертного забезпечення протидії організованій злочинності: досвід та практика; інформаційне забезпечення правоохоронних органів у боротьбі з організованою злочинною діяльністю; інноваційні технології та сучасні методи розслідування у протидії організованій злочинності; кримінально-правові, кримінально-процесуальні та кримінологічні проблеми забезпечення протидії організованій злочинності.

Висловлюємо вдячність усім авторам за активну участь, якісний науковий матеріал та високий рівень академічної доброчесності.

Матеріали викладені в авторській редакції.

Відповідальність за зміст, наукову новизну, коректність цитування та достовірність фактичного матеріалу несуть автори.

UDC 340.6:343.9.022 (062)

Recommended for publication by the decision of the Department of Criminalistics, Forensic Examinations and Polygraphology NU «OLA» (Pr. 9, November 24, 2025)
Recommended for publication by the decision of the Academic Council of ONDISE (Pr. 9, December 1, 2025)

Expert Support in the Investigation of Organized Crime: International Experience and National Practice: Proceedings of the International Scientific and Practical Conference (Odesa, 27 November 2025) / [Organizing Committee: S. Kivalov, M. Arakelyan, O. Cataraga, D. Kishko, D. Kolodin, A. Kolodina, L. Arkusha et al.]; National University «Odesa Law Academy», Department of Criminalistics, Forensic Examinations and Polygraphology; National Centre of Judicial Expertise of the Ministry of Justice of the Republic of Moldova; Odesa Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine. Odesa:NU«OLA», 2025. 450 p.

The Proceedings contain papers presented at the International Scientific and Practical Conference «Expert Support in the Investigation of Organized Crime: International Experience and National Practice», which brought together over 100 scholars and practitioners from Ukraine and other European countries. The materials address urgent scientific and practical issues, such as expert support for combating specific types of organized crime; the use of specialized knowledge and expert support for investigating organized crime during armed conflict; international cooperation in forensic support for combating organized crime; information support for law enforcement in countering organized criminal activity; innovative technologies and modern investigative methods; and criminal law, criminal procedure, and criminological issues in ensuring effective counteraction to organized crime.

We express our sincere gratitude to all authors for their active participation, high-quality academic contributions, and strong adherence to academic integrity.

The materials are published in the authors' original versions.

Authors bear responsibility for the content, scientific novelty, accuracy of citations, and reliability of factual information.

Іван Старенький
старший судовий експерт лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем (обладнання) та засобів Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України,
м. Одеса, Україна
ORCID: https://orcid.org/0009-0004-2271-8512
електронна адреса: ivanstarenkii777@gmail.com

ДИНАМІЧНЕ ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ RACCOON STEALER

У тезах розглянуто практичний випадок дослідження шкідливого програмного забезпечення типу «Stealer», а саме «Raccoon Stealer». Наведено перелік програмних продуктів за допомогою яких проводиться динамічне дослідження.

Ключові слова: Raccoon Stealer, динамічне дослідження, оболонка PowerShell, віртуальне середовище.

Ivan Starenkiy
senior forensic expert of the laboratory for research of information technology objects, telecommunication systems (equipment) and means of the Odessa Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine, Odesa, Ukraine

DYNAMIC RESEARCH OF RACCOON STEALER MALWARE

The theses examine a practical case of analyzing malicious software of the Stealer type, specifically Raccoon Stealer. A list of software tools used to perform dynamic analysis is provided

Keywords: Raccoon Stealer, Malware, Dynamic Research, Operating System, Program Shell «PowerShell», Isolated Virtual Environment.

Будь яке дослідження потенційного шкідливого програмного забезпечення (ШПЗ) повинно виконуватися в два етапи: перший, це статичний аналіз об'єкту дослідження, в процесі виконання якого збирається максимальний обсяг даних щодо шкідливого зразку, що в подальшому допоможе визначити вектор подальшого дослідження даного шкідливого зразку, і другий етап – динамічне дослідження.

Динамічне дослідження ШПЗ необхідно проводити в ізольованому віртуальному середовищі, аби запобігти вірогідним негативним наслідкам дії шкідливого зразку на операційну систему (ОС) робочої станції (РС), що в своїй перспективі можуть спричинити втрату доступу до робочого середовища ОС, або викликати виток інформації на віддалений С2-сервер (Command and Control)

зловмисників, або ж динамічне дослідження можна проводити на спеціально підготовленому для таких задач персональному комп'ютері (ПК), який після завершення кожного такого дослідження, програмним шляхом повертається в момент часу до початку динамічного дослідження, так би мовити, скидається до «заводських налаштувань».

В ході своєї професійної діяльності, автором було визначено наступний перелік програмних продуктів, які є найоптимальнішими для проведення динамічного дослідження зразків ШПЗ, це «Process Monitor» [1], «Process Hacker» [2], «Autoruns» [3], «Microsoft Network Monitor» [4], «Wireshark» [5].

Використання ПЗ «Process Monitor» (див. рис. 1) дозволить відслідковувати абсолютно всі процеси в середовищі ОС до, під час, та після динамічного дослідження зразку ШПЗ, що дозволить сформувати повну картину подій, до, та після ініціалізації об'єкту дослідження в системі.

1:40:29.6294140 PM	2.1.0-4.exe	624	TCP Reconnect	DESKTOP-30RF073:62594 -> k3s-agent-huge-hel-krj.k3s.alteox.app:http	SUCCESS
1:40:31.6294962 PM	2.1.0-4.exe	624	TCP Reconnect	DESKTOP-30RF073:62594 -> k3s-agent-huge-hel-krj.k3s.alteox.app:http	SUCCESS
1:40:31.6466036 PM	svchost.exe	1120	UDP Send	DESKTOP-30RF073:58146 -> 10.0.2.3:domain	SUCCESS
1:40:31.6771948 PM	svchost.exe	1120	UDP Send	DESKTOP-30RF073:58146 -> 10.0.2.3:domain	SUCCESS
1:40:31.7023522 PM	svchost.exe	1120	UDP Receive	DESKTOP-30RF073:58146 -> 10.0.2.3:domain	SUCCESS
1:40:35.6296037 PM	2.1.0-4.exe	624	TCP Reconnect	DESKTOP-30RF073:62594 -> k3s-agent-huge-hel-krj.k3s.alteox.app:http	SUCCESS
1:40:43.6300130 PM	2.1.0-4.exe	624	TCP Reconnect	DESKTOP-30RF073:62594 -> k3s-agent-huge-hel-krj.k3s.alteox.app:http	SUCCESS
1:40:49.6242175 PM	2.1.0-4.exe	624	TCP Disconnect	DESKTOP-30RF073:62594 -> k3s-agent-huge-hel-krj.k3s.alteox.app:http	SUCCESS

Рисунок 1 – Моніторинг процесів зразку ШПЗ в середовищі ПЗ «Process Monitor»

Використання ПЗ «Autoruns» дозволить встановити перелік ПЗ та процесів, що запускаються в фоновому режимі при початку роботи ОС, і ніяким чином візуально про себе не повідомляють.

Загально можна виділити два основних сценарії застосування ПЗ «Autoruns», це використання даного програмного продукту (ПП) в ізольованому віртуальному середовищі, в якому безпосередньо буде проводитися динамічне дослідження шкідливих зразків, та інший сценарій, який передбачає створення віртуальної машини з побітової копії носія інформації, в пам'яті якого було ініціалізовано запуск шкідливого файли, що в свою чергу спричинило до зараження системи ШПЗ.

За допомогою ПЗ «Microsoft Network Monitor», або «Wireshark», запущеного заздалегідь до моменту динамічного аналізу, можна відстежити мережеву активність тестового зразку, та встановити IP-адреси, до яких він буде звертатися, див. рис. 2.

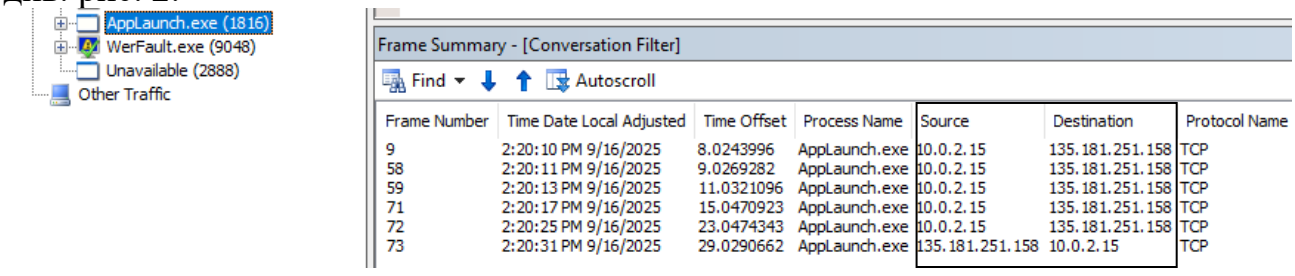


Рисунок 2 – Дослідження зразку ШПЗ за допомогою ПЗ «Microsoft Network Monitor»

Коли за допомогою ПЗ «Autoruns» та «Microsoft Network Monitor» вдається встановити процеси ШПЗ, а також відомості щодо мережевої активності, наступним кроком є використання ПЗ «Process Hacker» (див. рис. 3), або його аналогів, який дозволить встановити наявність або відсутність дочірніх процесів у шкідливого файлу.

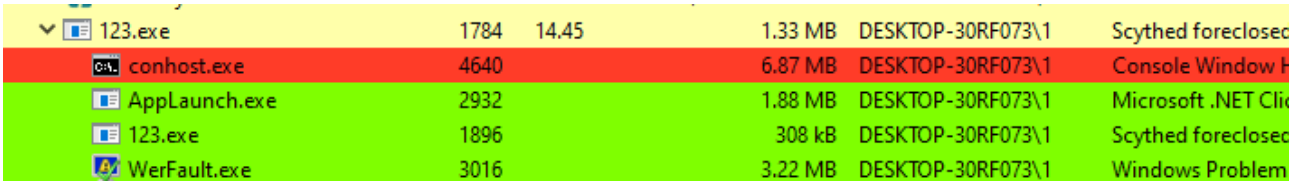


Рисунок 3 – Динамічне дослідження зразку ШПЗ
за допомогою ПЗ «Process Hacker»

Невід'ємною перевагою ПЗ «Process Hacker» є одна з його функціональних можливостей, що передбачає створення дампу пам'яті власноруч обраного процесу.

Ключовою перевагою зняття дампу пам'яті шкідливого процесу під час його динамічного дослідження, на противагу статичному аналізу, коли програмний код може бути зашифровано складними алгоритмами шифрування, дешифрування яких провести або вкрай складно, або навіть неможливо – є те, що під час свого виконання, ШПЗ взаємодіє з ОС в розпакованому, розшифрованому та робочому стані, що дозволяє в подальшому встановити з якими файлами, процесами, а також яку інформацію отримав, під час свого виконання, зразок ШПЗ від ОС.

Так, зі збереженого дампу пам'яті процесу «AppLaunch.exe», наведеного на рис. 3, за допомогою наведеної нижче команди для програмної оболонки «PowerShell» (успішність виконання якої потребує попереднього встановлення необхідних ПП), виконується пошук по ключовим словам (де «XXXXX», це перелік ключових слів, який вдалося встановити під час статичного та динамічного аналізів тестового зразку) серед збереженої в дампі пам'яті інформації:

```
    &  «$env:TEMP\Strings\strings64.exe»  -accepteula  -n  6  -u
C:\шлях_до_файлу_дампу_пам'яті\файл_дампу_пам'яті.dmp |
      Select-String -SimpleMatch -Pattern 'XXXXX'
```

Використання для свого пошуку наступного переліку ключових слів «txt», «.exe», «tlgrm», «wallet», «dscrd_», «sqlite», «login», «Content-Type», «User Data», «SELECT», «stable», «machineId», ««encrypted_key»:»«, «MachineGuid», «local state», «NSS_Shutdown», «PK11_GetInternalKeySlot», «PK11_Authenticate», «PK11SDR_Decrypt», «webextension@metamask.io», «http://», «GdipGetImageEncoders»,

«GdipGetImageEncodersSize», «GdipCreateBitmapFromHBITMAP», «GdipSaveImageToFile», «BaseNamedObjects», «lnk» та «RAM:», дозволить встановити відомості щодо наступних функціональних можливостей зразку ШПЗ:

1. Взаємодія з WEB-оглядачами;
2. Взаємодія з криптогаманцями/WEB-розширенням;
3. Взаємодія з мережою Інтернет;
4. Взаємодія з месенджарами;
5. Створення звітних файлів;
6. Ідентифікація жертви;
8. Можливість робити знімки екрану PC.

Ключовими моментами з наведеного вище переліку функціональних можливостей ШПЗ типу «Stealer» – є виявлення свідчень щодо файлів з розширенням «*.txt», а саме «passwords.txt», «cookies.txt», «ffcookies.txt», «autofill.txt», «CC.txt», що вказує на функціональну можливість ШПЗ обробляти інформаційне наповнення накопичувача PC, та узагальнювати виявлені «цільові дані» в звітні файли, та надсилати їх на C2-сервер, IP-адресу якого було встановлено під час динамічного дослідження.

Перелік використаних джерел:

1. Process Monitor. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon.
2. Process Hacker. URL: https://systeminformer.sourceforge.io/
3. Autoruns. URL: https://learn.microsoft.com/ru-ru/sysinternals/downloads/autoruns.
4. Microsoft Network Monitor. URL:https://www.microsoft.com/en-us/download/details.aspx?id=4865.
5. Wireshark. URL: https://www.wireshark.org/.