УДК 004.056:343.98

А. Р. Магденко
І. О. Бондаренко

СУДОВО-ЕКСПЕРТНЕ ДОСЛІДЖЕННЯ АРТЕФАКТІВ ЕНЕРГОЗАЛЕЖНОЇ ПАМ'ЯТІ (RAM) ПРИ РОЗСЛІДУВАННІ ІНЦИДЕНТІВ КОМПРОМЕТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

У роботі розглянуто проблема судово-експертного дослідження енергозалежної пам'яті (RAM) під час розслідування кіберзлочинів. Проведено аналіз поширених кібератак, таких як: поширення безфайлового шкідливого програмного забезпечення та методів виконання коду безпосередньо в оперативній пам'яті (In-Memory Execution). При цьому, застосування методів комп'ютерної криміналістики, які зосереджені виключно на енергонезалежних носіях, виявляються недостатніми для протидії таким кіберзагрозам.

Представлено різні способи отримання електронних доказів з урахуванням принципу пріоритетності збору даних відповідно до рівня їхньої волатильності. Крім того, описано метод виявлення інцидентів безпеки шляхом аналізу дескрипторів віртуальних адрес (VAD). Запропонований метод дає змогу виявляти аномалії у розподілі пам'яті, які свідчать про застосування методів приховування процесів і несанкціонованого впровадження шкідливого коду.

Обґрунтовано необхідність реконструкції мережевих з'єднань та вилучення залишкових криптографічних даних з некатегоризованих областей пам'яті. Таким чином, стандартизація протоколів криміналістичного аналізу волатильної пам'яті є необхідною передумовою забезпечення процесуальної допустимості та достовірності електронних доказів у кримінальних провадженнях.

Ключові слова: *цифрова криміналістика, енергозалежна пам'ять, електронні докази, безфайлове шкідливе програмне забезпечення, дескриптори віртуальних адрес, криптографічне гешування, ін'єкція коду, криміналістичний карвінг пам'яті.*

Abstract

This paper examines the issue of forensic analysis of volatile memory (RAM) during cybercrime investigations. It analyzes common cyberattacks, such as the spread of fileless malware and methods of executing code directly in RAM (in-memory execution). At the same time, the application of computer forensics methods that focus exclusively on non-volatile storage media proves insufficient to counter such cyber threats.

The paper presents various methods for obtaining electronic evidence, taking into account the principle of prioritizing data collection based on volatility. In addition, a method for detecting security incidents using the analysis of virtual address descriptors (VAD) is described. This method detects anomalies in memory allocation that indicate the use of process obfuscation techniques and the unauthorized injection of malicious code.

The necessity of reconstructing network connections and extracting residual cryptographic data from uncategorized memory regions is justified. Thus, the standardization of protocols for the forensic analysis of non-volatile memory is a necessary prerequisite for ensuring the admissibility and reliability of electronic evidence in criminal cases

Keywords: *digital forensics, volatile memory, electronic evidence, fileless malware, virtual address descriptors, cryptographic hashing, code injection, forensic memory carving.*

Вступ

Розробка методів компрометації інформаційних систем вимагає постійної адаптації методів, які використовуються в комп'ютерній криміналістиці. Для сучасних кіберзагроз характерним є використання складних безфайлових архітектур шкідливого програмного забезпечення. Такі алгоритми та атаки передбачають виконання шкідливого коду безпосередньо в оперативній пам'яті, без створення виконуваних файлів на диску цільової системи, що ускладнює їх виявлення [1]. Така зміна парадигми в тактиці кіберзлочинності виявила критичний недолік традиційних методів криміналістичного аналізу, які історично були зосереджені переважно на дослідженні енергонезалежних носіїв інформації (HDD, SSD).

Відповідно, дослідження волатильної пам’яті (RAM) трансформується з факультативного етапу технічного реагування на кіберінциденти у фундаментальну складову формування належної та юридично значущої доказової бази. З огляду на динамічний характер оперативної пам’яті, будь-яка затримка в екстракції даних або некваліфіковане втручання призводить до безповоротної втрати криміналістично значущої інформації. Це робить аналіз RAM одним із найскладніших і водночас найпріоритетніших напрямів сучасної цифрової криміналістики [2].

Результати дослідження

Процес криміналістичного дослідження артефактів енергозалежної пам’яті концептуально розпочинається з етапу прецизійної екстракції даних, що вимагає суворого дотримання принципу черговості збору доказів залежно від їхньої мінливості (Order of Volatility) [1].

Оскільки оперативна пам’ять є найбільш динамічним середовищем інформаційної інфраструктури, процедура створення криміналістичної копії (дампу) об’єктивно пов’язана з неминучим втручанням у поточний стан цільової операційної системи. Запуск будь-якого процесу безпосередньо на скомпрометованій машині неминуче призводить до перезапису певного обсягу волатильних даних, що зумовлює ризики знищення криміналістично значущих артефактів.

Для мінімізації цього деструктивного впливу використовуються виключно вузькоспеціалізовані програмні засоби екстракції, які функціонують на рівні ядра операційної системи. Такі драйвери ядра забезпечують прямий доступ до фізичного адресного простору в обхід стандартних інтерфейсів прикладного програмування (API), що дозволяє суттєво зменшити так званий «слід у пам’яті» (Memory Footprint). Процесуальна допустимість отриманих результатів у кримінальному провадженні безальтернативно потребує імплементації алгоритмів криптографічного гешування (переважно SHA-256) безпосередньо під час формування образу пам’яті, що гарантує беззаперечну цілісність цифрового об’єкта та юридично фіксує його незмінність з моменту вилучення [2].

Методологія дослідження енергозалежного середовища не обмежується виключно фізичною оперативною пам’яттю (RAM), а обов’язково поширюється на системні файли, що архітектурно виконують функцію її розширення на енергонезалежних носіях. До таких об’єктів належать файли підкачки (pagefile.sys, swapfile.sys) та файл гібернації (hiberfil.sys). У процесі функціонування операційної системи алгоритми керування пам’яттю переміщують неактивні сторінки пам’яті з RAM у файл підкачки для звільнення ресурсів. Відповідно, дослідження цих сторінкових файлів дозволяє ретроспективно відновити фрагменти шкідливого коду, криптографічні ключі або фрагменти текстової комунікації, які вже були витіснені з фізичної пам’яті. Файл гібернації, своєю чергою, є стисненим зліпком повного стану оперативної пам’яті на момент переходу системи у режим сну, що надає судовому експерту унікальну можливість проаналізувати статичний контекст виконання процесів у конкретний історичний момент часу до виникнення інциденту компрометації [4].

Безпосередній експертний аналіз структури збереженого дампу пам’яті фокусується на глибинній реконструкції системних структур операційної системи. Першочерговим завданням є відтворення ієрархії активних, прихованих та завершених процесів. Сучасне складне шкідливе програмне забезпечення активно застосовує техніки прямого маніпулювання об’єктами ядра (Direct Kernel Object Manipulation, DKOM). Шляхом модифікації системних структур шкідливий процес видаляє власні дескриптори з двонаправленого списку (наприклад, ActiveProcessLinks), стаючи абсолютно невидимим для стандартних інструментів моніторингу, але при цьому його потоки продовжують виконуватися процесором [3]. Для виявлення таких аномалій застосовується криміналістичний карвінг пам’яті (Memory Carving), який полягає у послідовному скануванні всього адресного простору на наявність специфічних пулових тегів, що відповідають структурам керування процесами (EPROCESS у системах Windows). Такий незалежний від API підхід дозволяє експертам ідентифікувати приховані процеси-руткіти та верифікувати реальний, а не сфальсифікований стан скомпрометованого середовища.

Дослідження передбачають детальний аналіз описів віртуальних адрес, які формують деревоподібну структуру, що використовується для керування адресним простором кожного процесу. Аналіз VAD дозволяє ідентифікувати сторінки пам’яті з правами доступу, що мають одночасні права на запис та виконання (PAGE_EXECUTE_READWRITE).

Виявлення таких сегментів пам’яті, які не мають відповідного зворотного відображення на легітимний виконуваний файл на диску (Unbacked Memory Pages), є надійним індикатором використання технік приховування шкідливих сегментів коду, таких як Process Hollowing (підміна тіла

легітимного процесу) або несанкціонованих ін'єкцій динамічних бібліотек (DLL Injection) [2]. Встановлення факту ін'єкції дозволяє експерту екстрагувати розпакований (дешифрований) шкідливий код безпосередньо з пам'яті для подальшого реверс-інжинірингу.

Окремим вектором судово-експертного дослідження є реконструкція мережевої активності та екстракція криміналістично значущих автентифікаційних даних. Аналіз мережевих артефактів у волатильній пам'яті, зокрема сканування пулів пам'яті на наявність структур, пов'язаних із кінцевими точками TCP/UDP, дає змогу відновлювати таблиці маршрутизації та ідентифікувати активні або нещодавно завершені мережеві з'єднання незалежно від спроб руткітів приховати ці дані на рівні мережевого стека. Це має критичне значення для встановлення IP-адрес командно-контрольних серверів (C&C), з якими взаємодіяв шкідливий код.

Водночас глибокий аналіз пам'яті процесу локальної підсистеми автентифікації (Local Security Authority Subsystem Service, LSASS) дає можливість екстрагувати криптографічні геші паролів користувачів (NTLM) та квитки автентифікації, що беззаперечно вказує на вектори латерального переміщення зловмисників усередині корпоративної мережі [3]. Крім того, сканування невідкатегорованих пулів пам'яті з використанням алгоритмів розрахунку ентропії дозволяє виявляти тимчасово збережені симетричні ключі шифрування (наприклад, ключі алгоритмів AES чи RSA, згенеровані програмами-вимагачами), екстракція яких до моменту повного знеструмлення системи залишається єдиним можливим механізмом відновлення зашифрованої цифрової інформації [4].

Висновки

Отже, результати цього дослідження демонструють, що інтеграція методів судово-експертного аналізу RAM у стандартні процедури розслідування інцидентів кібербезпеки більше не є варіативною, а стала необхідною складовою діяльності сучасних правоохоронних органів . Швидка еволюція архітектур шкідливого програмного забезпечення, зокрема поширення безфайлових загроз і застосування передових методів прямого маніпулювання об'єктами ядра (DKOM) , ставить під сумнів ефективність традиційних судово-експертних методів, що ґрунтуються виключно на статичному аналізі енергонезалежних носіїв інформації.

Оперативна пам'ять стала ключовим джерелом електронних доказів, яке містить критично важливі сліди хакерських атак, зокрема фрагменти шкідливого програмного забезпечення, ін'єкції коду з криптографічними залишками, ключі сеансів та хеші автентифікації.

Стандартизація протоколів аналізу даних із використанням спеціалізованих драйверів ядра, а також забезпечення цілісності образу пам'яті шляхом застосування криптографічних алгоритмів хешування є необхідними умовами верифікації цифрових доказів у судових процесах [5].

Крім того, детальний аналіз системних структур, таких як віртуальні адресні дескриптори та структури керування процесами (EPROCESS), надає судово-експертним службам ефективні інструменти для виявлення навіть найскладніших векторів атак, включаючи приховану діяльність високотехнологічних груп, таких як Advanced Persistent Threats (APT).

Подальший розвиток експертизи у сфері криміналістичного аналізу цифрових доказів, у поєднанні з упровадженням сучасних міжнародних стандартів управління цифровими доказами, сприятиме переходу від реактивної моделі реагування на кібератаки до проактивної парадигми кіберзахисту. Такий підхід, орієнтований на раннє виявлення та нейтралізацію кіберзагроз є важливим чинником забезпеченні кіберстійкості та комплексної інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Козицька О. Щодо поняття електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 8. С. 418–421. DOI: https://doi.org/10.32782/2524-0374/2020-8/103.

2. Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. Вісник кримінального судочинства. 2023. № 1–2. С. 42–53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53.

3. Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2024. Вип. 85, ч. 4. С. 63–70. DOI: https://doi.org/10.24144/2307-3322.2024.85.4.9.

4. Музиченко О. В., Карандась М. В. Електронні докази як джерела доказів у межах кримінального провадження: судова практика та нормативне регулювання інших процесуальних кодексів України. Київський часопис права. 2022. № 2. С. 170–176. DOI: https://doi.org/10.32782/klj/2022.2.25.

5. Караман К.В. Сучасна парадигма криміналістичного значення цифрових слідів у кримінальному провадженні. Вісник кримінологічної асоціації України. 2025. № 2 (35). Частина 1. С. 224–233. DOI: https://doi.org/10.32631/vca.2025.2.16.

Магденко Анастасія Романівна – студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anastasiiamahdenko@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна –*** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Mahdenko Anastasiia R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiiamahdenko@gmail.com

Supervisor: ***Bondarenko Iryna O. –*** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua