Практичне оцінювання засобів виявлення та аналізу альтернативних потоків даних *NTFS*

Віталій Носов
професор кафедри протидії кіберзлочинності, навчально-науковий інститут № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна,
ORCID: https://orcid.org/0000-0002-7848-6448, e-mail: vitnos@univd.edu.ua

Роман Стецик
курсант, навчально-науковий інститут № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна, ORCID: https://orcid.org/0009-0009-1263-184X,
e-mail: romanstetsyk06@gmail.com

Іван Цуркан
курсант, навчально-науковий інститут № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна, ORCID: https://orcid.org/0009-0009-6621-4056, e-mail: curivan82@gmail.com

Здійснено практичне оцінювання засобів виявлення та аналізу альтернативних потоків даних файлової системи NTFS.
Ключові слова: *цифрова криміналістика; NTFS; альтернативні потоки даних.*

Practical Evaluation of Tools for Detecting and Analyzing Alternative NFTS Data Streams

Vitalii Nosov, Roman Stetsyk, Ivan Tsurkan

The paper outlines a practical evaluation of tools for detecting and analyzing alternative data streams of the NTFS file system.
Keywords: *digital forensics; NTFS; alternative data streams.*

Файлова система *NTFS* відрізняється від інших файлових систем наявністю так званих альтернативних потоків даних (англ. *Alternate Data Streams*, *ADS*), які дають змогу зберігати додаткову інформацію разом з основним умістом файлу, не змінюючи його основної структури. Повне позначення потоку файлу має формат <filename>:<stream name>:<stream type>.

Усі файли в системі *NTFS* за замовчуванням містять як мінімум один (основний) потік даних, який є видимим для файлових менеджерів і позначається як <filename>::$DATA [1].

Операційна система *Windows* застосовує *ADS* для зберігання додаткової системної інформації про файл / каталог. Користувач може додати незліченну кількість невидимих іменованих потоків даних до файлу / каталога, і тоді додатковий потік даних, наприклад з іменем bar у файлі sample.txt, позначається як sample.txt:bar:$DATA. Альтернативні потоки не відображаються файловими менеджерами, доступні тільки через командний рядок і в разі запуску виконуваного потоку відображаються іменем батьківського файлу [2].

Наявність *ADS* дає змогу зловмисникові приховувати чутливі дані або шкідливе програмне забезпечення як у власній системі, так і в системі, до якої отримано несанкціонований доступ.

Для виявлення можливих слідів (цифрових доказів) злочинної діяльності необхідно досліджувати наявні *ADS* у комп'ютерній системі. Сьогодні для криміналістичного дослідження *ADS* можна застосувати такі програмні засоби: *AlternateStreamView*, *Stream Detector*, *ADS Manager*, *Streams*, *StreamArmor*, *Autopsy*. Для їх практичного оцінювання в ОС *Windows 11 Pro* у програмі віртуалізації *Oracle VirtualBox* розгорнуто віртуальну машину *Windows 10 Pro* із жорстким диском 37 ГБ, де створено 8 користувацьких файлів із різною кількістю *ADS* і відредаговано наявний *ADS* в одному системному файлі (див. табл. *1*). Для створення *ADS* застосовували різні типи файлів з однаковими розмірами: текстове повідомлення — 16 Байт, зображення — 5570 Байт, python скрипт — 41 228 Байт, аудіо — 11 021 413 Байт, відео — 1 857 892 Байт, архів *RAR* — 54 Байт, виконуваний файл — 1310 Байт. Файл «hide7» видалений у кошик, файл «hide8» зашифрований на рівні файлової системи [3].

Таблиця 1

Перелік і характеристики тестових файлів з *ADS*

№	Назва файлу	Місце знаходження файлу	К-ть *ADS*	Назва *ADS*	Уміст *ADS*
1	hide1	C:*Windows*	1	file1_1	Текстове повідомлення
2	hide2	C:\Program Files*Windows* Multimedia Platform	2	file2_1, file2_2	Фото, відео
3	hide3	C:\Program Files*Windows*Apps	3	file3_1, file3_2, file3_3	Виконуваний файл, python скрипт, архів *RAR*
4	hide4	C:\Program Files (x86)*Windows* Photo Viewer	4	file4_1, file4_2, file4_3, file4_4	Фото, текстове повідомлення, архів *RAR*, виконуваний файл

Завершення табл. 1

№	Назва файлу	Місце знаходження файлу	К-ть *ADS*	Назва *ADS*	Уміст *ADS*
5	hide5	C:\ProgramData\Packages\ Microsoft.MicrosoftEdge. Stable_8wekyb3d8bbwe\ S-1-5-21-3949679530-4065500778-521339517-1001\SystemAppData	5	file5_1, file5_2, file5_3, file5_4, file5_5	Аудіодоріжка, python скрипт, фото, текстове повідомлення, архів *RAR*
6	hide6	C:\ProgramData\USOShared\Logs\ User	6	file6_1, file6_2, file6_3, file6_4, file6_5, file6_6	Відео, фото, аудіодоріжка, python скрипт, виконуваний файл, архів *RAR*
7	*hide7*	Видалений	2	file7_1, file7_2	Відео, аудіодоріжка
8	*hide8*	C:\Users\User\Desktop	2	file8_1, file8_2	Виконуваний файл, python скрипт
9	hide9	C:\Users\User\Downloads	1	Zone. Identifier	Текстове повідомлення

У процесі дослідження за допомогою *FTK Imager* [4] спочатку створено образ жорсткого диска цільової системи з ОС *Windows 10 Pro*, а потім за допомогою *OSF Mount* [5] отримано образ, змонтований як логічний диск.

Результати пошуку *ADS* зазначеними програмними засобами наведено в табл. 2. Видалений файл «hide7» мав змінену назву, а імена його потоків залишились незмінними, уміст потоків «file8_1», «file8_2» зашифрувалися разом із батьківським файлом.

Таблиця 2

Результати виявлення *ADS* різними програмними засобами

Параметр	**Alternate-StreamView** [6]	**Stream Detector** [7]	**ADS Manager** [8]	**Streams** [9]	**Stream Armor *** [10]	**Autopsy** [11]
Час пошуку (хв)	5	33	9	3	13	0.1
Кількість виявлених користувацьких ADS	18	24	5	24	22	26

* Stream Armor працює тільки в ОС *Windows 10*.

У підсумку серед протестованих програмних засобів можна виокремити *Autopsy*, який допомагає працювати з образом диска без монтування та виявляти системні *ADS*,— ідентифіковано приблизно 14000 *ADS*. *Autopsy* не має окремої опції пошуку користувацьких *ADS*, проте дає змогу це

здійснити за допомогою опцій: «*File Search by Attributes*», «*Keyword Search*» і «*Keyword Lists*». «*File Search by Attributes*» дає змогу відображати всі файлові потоки системи, увівши у полі «*Names*» символ «:», який є забронюваним у файлові системі *NTFS*, а фільтрацію здійснювати за допомогою фільтрів: «*Size*», «*Extension*», «*MIME Type*». Інструменти «*Keyword Search*» і «*Keyword Lists*» сприяють здійсненню пошуку за ключовими словами або списками ключових слів у вмісті файлу, що допомагає аналізувати вміст *ADS*.

Перелік джерел посилання

1. 5.1 *NTFS* Streams / AI Skills Challenge. 12/14/2021. URL: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/c54dec26-1551-4d3a-a0ea-4fa40f848eb3 (дата звернення: 28.09.2024).
2. *Windows* ::DATA Alternate Data Stream / OWASP Foundation. URL: https://owasp.org/www-community/attacks/*Windows*_alternate_data_stream (дата звернення: 28.09.2024).
3. File Encryption / AI Skills Challenge. 01/13/2023. URL: https://learn.microsoft.com/en-us/windows/win32/fileio/file-encryption (дата звернення: 28.09.2024).
4. Create Forensic Images with Exterro *FTK Imager* / Exterro. URL: https://www.exterro.com/digital-forensics-software/ftk-imager (дата звернення: 28.09.2024).
5. OSFMount / PassMark Software. URL: https://www.osforensics.com/tools/mount-disk-images.html (дата звернення: 28.09.2024).
6. AlternateStreamView v1.58 — View/Copy/Delete *NTFS* Alternate Data Streams Copyright (c) 2009—2023 Nir Sofer / Nirsoft. URL: https://www.nirsoft.net/utils/alternate_data_streams.html (дата звернення: 28.09.2024).
7. Stream Detector v1.4 / AppsVoid. URL: https://www.appsvoid.com/products/stream-detector/ (дата звернення: 28.09.2024).
8. Brant D. *ADS* Manager / Dmitrybrant. URL: https://dmitrybrant.com/adsmanager (дата звернення: 28.09.2024).
9. Streams v1.6 / AI Skills Challenge. 03/23/2021. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/streams (дата звернення: 28.09.2024).
10. StreamArmor / SecurityXploded. URL: https://securityxploded.com/streamarmor.php (дата звернення: 28.09.2024).
11. Download *Autopsy* for free / *Autopsy* Digital Forensics. URL: https://www.autopsy.com/ (дата звернення: 28.09.2024).