Аналіз місць приховування даних у файловій системі NTFS

Баришев Ю. В.[1], Поворознюк О.О.[2]

[1]К. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця

[2]Студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, e-mail: povarss@outlook.com.

***Анотація* — Дослідження присвячено огляду та аналізу місць приховування інформації на комп'ютерах з файловою системою NTFS. Визначено будову файлових потоків, властивості та можливі методи, за допомогою яких альтернативні потоки даних використовуються, як контейнери даних для вбудовування інформації. Досліджено атрибути файлової системи NTFS в яких можна приховувати дані та виділено альтернативні файлові потоки, які найбільш перспективні для розробки програмного засобу для приховування даних.**

Ключові слова: файлова система, стеганографія, файлові потоки , NTFS.

Analyses of data hiding places at the NTFS file system

Baryshev Y.V.[1], Povoroznyuk O.O.[2],

[1]PhD (ukr), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine

[2]Student, Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: povarss@outlook.com.

***Abstract* - The research is devoted to the review and analyses of information hiding places at computers with the NTFS file system. Defined file structure of the flow properties and possible methods by which alternate data streams are used as containers for embedding data information. Studied the attributes of NTFS file system in which to hide data and alternate file streams that are more promising for the development of software. Advantages and disadvantages of alternative data streams and attributes of the file system NTFS.**

Keywords: file system, steganography, file stream, NTFS.

Вступ

Створення надійного захисту інформації від несанкціонованого доступу є однією з найдавніших і невирішених до теперішнього часу проблем [1, 2]. Дана проблема актуальна, як для користувачів ПК, які хочуть приховати свої особисті документи, програми та інші дані, так і в ході розробки специфічного програмного забезпечення, коли, необхідно запускати виконуваний файл, прихований від користувачів комп'ютера.

Приховані елементи використовуються для різних цілей. По-перше, Windows сама приховує низку елементів для того, щоб у разі недбалих дій не пошкодити важливі елементи. По-друге, користувачі комп'ютера приховують папки з міркувань безпеки та збереження особистої інформації. Варто іншому користувачеві включити відображення прихованих файлів, то ні про яку захищеності немає сенсу говорити [1] .

Основною метою досліджень є аналіз місць приховування інформації в файловій системі NTFS. В ході розробки проекту досліджено і проаналізовано підходи до вирішення проблеми приховування файлів, а саме використання атрибутів та файлових потоків файлової системи NTFS.

Дані в альтернативних потоках не видно неозброєним оком, підключенням іншої ОС чи використанням безпечного режиму. Існування додаткових потоків звичайним користувачам мало відомі. Однак, в світі комп'ютерної безпеки вони отримали певне поширення. Зловмисники використовують Alternative Data Stream (ADS) для зберігання файлів на зламаних комп'ютерах, іноді використовуються вірусами й іншим шкідливим

ПЗ. Справа в тому, що ці потоки не переглядаються звичайними методами [3].

На альтернативні потоки даних не завжди звертають увагу , до того ж не всі антивіруси за замовчуванням переглядають потоки в пошуках шкідливого програмного забезпечення, тому цей метод є актуальним для реалізації.

Аналіз атрибутів NTFS, для вбудовування даних

Всі атрибути можуть бути викликані, як потік байтів незалежно від того, чи є вони резидентними або нерезидентними. В табл. 1 наведено перелік атрибутів в яких можна приховувати дані та в яких не можна приховувати, або якщо приховати то робота файлової системи не буде працювати належним чином [6].

Таблиця 1 – Результат аналізу атрибутів, для вбудовування даних

Системні файли	**Назва файлу**	**Результати аналізу**
Головна таблиця файлів	$MFT	Системний файл не підлягає зміні
Копія перших 16 записів MFT	$MftMirr	Системний файл не підлягає зміні
Лог-файл	$ LogFile	Системний файл не підлягає зміні
Обсяг даних	$Volume	Системний файл не підлягає зміні
Визначення атрибутів	$AttrDef	Вбудовування даних можливе
Кореневий каталог	$	Системний файл не підлягає зміні
Відомості про зайнятість кластерів диску	$Bitmap	Системний файл не підлягає зміні
Завантажувальний сектор	$Boot	Системний файл не підлягає зміні
Биті кластери тому	$BadClus	Вбудовування даних можливе
Файл безпеки	$Secure	Системний файл не підлягає зміні
Таблиця співставлення імен	$Upcase	Системний файл не підлягає зміні
Розширення файлу NTFS	$Extend	Слабкий захист доступу
Зарезервовані		

Атрибути є файлами , але відкрити їх звичайним способом (наприклад за допомогою функцій NtOpenFile або NtCreateFile) не можна . Навіть отримавши в права адміністратора, доступ до них виявляється неможливий , оскільки для них Ntfs.sys (драйвер файлової системи NTFS) завжди повертає статус помилки STATUS ACCESS DENIED. У Ntfs.sys існують дві змінні, які впливають на його поведінку : NtfsProtectSystemFiles і NtfsProtectSystemAttributes . За замовчуванням, значенням обох цих змінних TRUE .

Якщо змінній NtfsProtectSystemAttributes привласнити значення FALSE (за допомогою налагоджувана), то, використовуючи імена в форматі «Файл :: $ STANDARDJNFORMATION » , можна отримати доступ до атрибутів системи (зокрема до стандартних інформаційних атрибутів). Якщо привласнити значення FALSE змінної NtfsProtectSystemFiles то можна буде відкрити спеціальні файли. Отже за допомогою налагоджувача, потрібно змінити значення в цих змінних, а далі, використовуючи атрибути в яких дозволено вбудовування (див. таб.1), приховувати потрібні дані.

Аналіз альтернативних потоків даних NTFS, для вбудовування інформації

В NTFS файли розглядаються, як набір атрибутів (розширених, резедентних, нерезидентних) та файлових потоків, які в свою чергу містять в собі головний файловий потік та певну кількість додаткових потоків данних. Тобто всередені одного файлу можуть бути приховані інші, але користувачеві доступний лише головний потік даних, в якому зберігається вміст основного файлу. Додаткові потоки не відображаються в списку каталогів чи вмісту файлу. Тому цю функцію можна використовувати для приховування даних без зміни їхнього вихідного розміру[2].

ADS це мало відома особливість файлової системи NTFS для Windows, яка забезпечує можливість поміщати дані в існуючі файли і папки, не втручаючись до їхньої функціональності і розміру. Будь-який такий потік, пов'язаний з файлом або папкою не відображається при перегляді за допомогою звичайних утиліт, таких, як провідник Windows, команда DIR або будь-які інші інструменти браузера файлів. Він використовується операційною системою і іншими додатками для зберігання додаткової інформації (наприклад перелік інформації) для файлу. Навіть 'Internet Explorer' додає потік з ім'ям 'Zone.Identifier' для кожного файлу, завантаженого з Інтернету.

Зловмисники використовують цей метод, щоб таємно зберігати свої руткіти в інфікованій

системі, не будучи виявленим. Наприклад, відомий руткіт під назвою “Mailbot.AZ” або “Backdoor.Rustock.A” використовується, щоб приховати свій файл драйвера в папці system32 (C: \ Windows \ system32) у вигляді потоку '18467'.

Додатки можуть створювати додаткові потоки і отримувати доступ до потоків, посилаючись на їх імена. Ця можливість дозволяє пов'язувати дані, які будуть управлятися як єдине ціле. Наприклад, графічна програма може зберігати мініатюрне зображення точкового малюнка в імені потоку даних всередині файлу NTFS, що містить зображення. В іменовані потоки даних можна приховувати певну кількість інформації, а саме стільки скільки доступно вільного об'єму на томі файлової системи. Іменовані потоки помітні тільки файловій системі NTFS, це забезпечує цілісність даних щодо, перенесення файлів з вбудованими файловими потоками на інші файлові системи , наприклад FAT.

Властивості файлових потоків:

- потік даних може містити в собі будь-який тип файлу;
- системи резервного копіювання підтримують приховані потоки. При відновленні системи потоки даних залишаються незмінними;
- користувач може створити потік даних за допомогою спеціально розробленого програмного забезпечення або командного рядка.
- при введенні даних в прихований потік , вказаний розмір файлу (тобто розмір в провіднику Windows) не збільшується. Проте, обсяг пам'яті, доступний на диску зменшується;
- під час спроби отримати доступ до прихованого потоку на інших файлових системах, з'являється повідомлення про помилку [4].

З точки зору NTFS кожен файл представлений, як набір атрибутів таких, як ім'я файлу, інформація, дані та інші. Кожен атрибут ідентифікований кодом типу атрибута і необов'язково ім'ям атрибута [5].

Якщо атрибути файлу можуть знаходиться всередині записів головної файлової таблиці MFT (Master File Table), вони називаються резидентними атрибутами. Якщо файл занадто великий, щоб розташовуватись в записах файлу MFT, він називається нерезидентним [2].

Нерезидентні атрибути займають один або кілька пробігів (безперервна лінійна область на диску) дискового простору в іншому місці тому, відповідно тоді з'являється додатковий простір на диску, який можна використати для вбудовування даних.

ВИСНОВКИ

Отримані результати, які отримані в результаті дослідження показують можливі методи приховування даних в файловій системі NTFS.

А, саме приховувати дані використовуючи файлові потоки або атрибути NTFS. Результати проведених досліджень визначають ефективність та практичну спроможність використання запропонованих методів для приховування. В атрибутах файлової системи NTFS дозволяється вбудовування, але є певні недоліки. Кількість інформації для вбудовування невелика, тому, що місце виділене для атрибутів файлової системи обмежене. Інший метод для приховування перспективніший і полягає у вбудовуванні інформації в альтернативні файлові потоки. Максимальна кількість інформації залежить від кількості вільного місця на диску, що надає даному методу перевагу над вбудовування в структуру записів головної таблиці файлів.

ЛІТЕРАТУРА REFERENCES

[1] Кастер Х. Основы Windows NT и NTFS / Хелен Кастер. – Москва: Русская Редакция, 1996. – 440 с.

[2] Руссинович М. Внутреннее устройство Microsoft Windows / М. Руссинович, Д. Соломон. – Питер: Питер, 2013. – 800 с..

[3] Артем Б. Исследование NTFS [Електронний ресурс] / Баранов Артем. – 2009. – Режим доступу до ресурсу: http://citforum.ru/operating_systems/windows/ntfs/.

[4] Vandome A. NTFS / A. Vandome, J. McBrewster, F. Miller. – Germany: International Book Marketing Service Ltd, 2009. – 224 с.

[5] Наик Д. Системы хранения данных в Windows. Серверные технологии хранения данных в среде Windows 2000 и Windows Server 2003 / Дайлип Наик., 2005. – 432 с. – (1).

[6] EC-Council. Computer Forensics: Hard Disk and Operating Systems / EC-Council. – Singapore: Cengage Learning, 2010. – 608 с. – (1).

[7] Meshram B. B. NTFS Alternate Data Streams Forensics Analysis [Електронний ресурс] / B. B. Meshram // B.B.Meshram. – 2012. – Режим доступу до ресурсу: http://www.ijert.org/view-pdf/276/ads-examiner-tool-for-ntfs-alternate-data-streams-forensics-analysis.

[8] Hughes J. The Stages of NTFS File Growth [Електронний ресурс] / Jeff Hughes. – 2009. – Режим доступу до ресурсу: https://blogs.technet.microsoft.com/askcore/2009/10/16/the-four-stages-of-ntfs-file-growth/.

[9] Berghel H. Phishing in Alternate Data Streams [Електронний ресурс] / H. Berghel, N. Brajkovska. – 2004. – Режим доступу до ресурсу: http://www.berghel.net/col-edit/digital_village/apr-04/dv_4-04.php.

[10] Sinofsky S. Building the next generation file system for Windows: ReFS [Електронний ресурс] / Steven Sinofsky // 2012 – Режим доступу до ресурсу: https://blogs.msdn.microsoft.com/b8/2012/01/16/building-the-next-generation-file-system-for-windows-refs/.