УДК 004.451.52.056.5

ПРИХОВУВАННЯ ОБ'ЄКТІВ ФАЙЛОВОЇ СИСТЕМИ В ОС КЛАСУ WINDOWS

ДуковД.Г., Шевченко О. Г.
Донецький національний технічний університет

Інформація – це один за найдорожчих об'єктів нашого сьогодення. Дуже часто вона має чи не найвищу ціну для людини. Тому є природнім той факт, що деяка інформація є конфіденційною і може бути доступна для обмеженого кола людей. Враховуючи те, що оперування інформацією в наш час здійснюється за допомогою персональних комп'ютерів актуальним стає питання про конфіденційність зберігання тієї чи іншої інформації в межах ПК. Одним з засобів вирішення цієї проблеми є приховування потрібної інформації. Оскільки збереження її на ПК виконується у вигляді об'єктів файлової системи (у вигляді файлів), то мова йде про приховування саме об'єктів файлової системи.

В даній роботі надається аналіз методів приховування об'єктів файлової системи та обґрунтовується вибір рішення з цього питання.

Існує декілька можливих способів приховування об'єктів файлової системи, серед яких слід виділити наступні:

- Приховування об'єктів на рівні структур конкретної файлової системи.
- Приховування об'єктів за допомогою перехоплення функцій ОС на рівні користувача (ring-3) для роботи із файловою системою та модифікації результатів, що повертають перехоплені функції.
- Приховування об'єктів за допомогою перехоплення функцій ОС на рівні ядра ОС (ring-0) для роботи із файловою системою та модифікації результатів, що повертають перехоплені функції.
- Приховування об'єктів за допомогою драйверу-фільтру файлової системи та перехоплення пакетів запиту вводу/виводу (IRP).

В методі приховування об'єктів на рівні структур конкретної файлової системи використовується прямий доступ до файлової системи. Приховування виконується із врахуванням особливостей конкретної файлової системи. Так, наприклад, для файлової системи типу FAT32 можна у таблиці кластерів помітити кластери об'єкту, що приховується, як помилкові , а у таблиці директорії видалити запис про об'єкт.

Переваги цього методу :

- дуже важко викрити об'єкт, що приховується.

Недоліки методу:

- залежність від типу файлової системи;
- неможливість роботи із прихованими об'єктами стандартними засобами ОС;
- необхідність реалізації власних засобів для доступу та роботи із прихованими об'єктами.

Метод приховування об'єктів за допомогою перехоплення функцій ОС на рівні користувача має деякі особливості. У ОС класу Windows для роботи із файлами використовуються наступні основні функції:

CreateFile, DeleteFile, FindFirstFile, FindNextFile, FindClose, ReadFile, WriteFile та ін.

Якщо необхідно просто приховати файловий об’єкт від користувача, то достатньо виконати перехоплення функцій, що виконують пошук, а саме: FindFirstFile, FindNextFile. При перехоплені FindFirstFile достатньо викликати справжню функцію FindFirstFile та перевірити результат. Якщо функція повернула об’єкт, що бажано приховати, то достатньо викликати функцію FindNextFile і повернути її результат, у іншому випадку можна просто повернути результат, що повернула справжня функція. При перехоплені функції FindNextFile також викликається справжня функція до тих пір, доки результат, що вона повертає є одним з об’єктів, що необхідно приховати. При такому методі все ж залишається можливість відкрити об’єкт, прочитати його вміст за допомогою стандартних функцій ОС (CreateFile, DeleteFile, ReadFile, WriteFile). Якщо такий доступ теж необхідно заборонити, достатньо перехопити функцію CreateFile, та перед відкриттям файлу перевіряти об’єкт, на необхідність приховування, чи заборони доступу.

Це є значно більш гнучкий метод приховування об’єктів файлової системи у порівнянні із попереднім.

Переваги цього методу наступні:

- відсутня залежність від типу файлової системи
- використання та перехоплення стандартних функцій для роботи із об’єктами файлової системи.

Недоліки методу :

- необхідність виконання перехоплення функцій для роботи із об’єктами файлової системи у кожному процесі системи, та у всіх нових, що будуть створюватися.
- можливість викривання, якщо звертатися напряму до функцій ядра ОС.

Метод приховування об’єктів за допомогою перехоплення функцій ОС на рівні ядра ОС також має свої особливості. У ОС класу Windows для роботи із файлами на рівні ядра використовуються наступні основні функції:

ZwCreateFile, ZwQueryDirectoryFile, ZwReadFile, ZwWriteFile та ін.

Якщо необхідно приховати файловий об’єкт від користувача, то достатньо виконати перехоплення функції, що виконує перелік об’єктів у визначеній директорії, а саме: ZwQueryDirectoryFile. При перехоплені ZwQueryDirectoryFile необхідно викликати справжню функцію ZwQueryDirectoryFile та перевірити результат. Звичайно ця функція повертає пов'язаний список структур, кожна з яких визначає один об’єкт у директорії. Якщо функція повернула список, що містить об’єкт, який бажано приховати, то потрібно трохи модифікувати цей список, видаливши з нього необхідну структуру і повернути результат. При такому методі все ж залишається можливість відкрити об’єкт, прочитати його вміст за допомогою стандартних функцій ОС (ZwCreateFile, ZwReadFile, ZwWriteFile). Якщо такий доступ теж необхідно заборонити, то достатньо, перехопити функцію ZwCreateFile, та перед відкриттям файлу перевіряти об’єкт, на необхідність приховування, чи заборони доступу.

Цей метод вимагає значно більше уваги та охайності при реалізації. Бо при хибній реалізації можна зробити систему дуже нестабільною, чи взагалі змусити аварійно зупинитись.

Переваги цього методу наступні:

- відсутня залежність від типу файлової системи;

- використання та перехоплення стандартних функцій для роботи із об’єктами файлової системи;
- централізований перехват функцій в одному місці (тобто немає потреби перехоплювати для кожного окремого процесу).

Недоліки методу :

- високі вимоги до кваліфікації фахівця;
- необхідність використання неофіційних та недокументованих засобів.

Четвертий метод, метод приховування об’єктів за допомогою драйверу-фільтру файлової системи та перехоплення пакетів запиту вводу/виводу (IRP) є найбільш гнучким. За роботу з файловими системами на рівні ядра ОС відповідають драйвери файлових систем, що створюють у системі пристрої для читання/запису/доступу до об’єктів файлової системи. ОС класу Windows XP підтримує багаторівневу організацію драйверів. Тобто між драйвером файлової системи, що працює із файловою системою безпосередньо, та тим хто, запитує інформацію по якомусь об’єкту файлової системи, може бути безліч проміжних драйверів-фільтрів. Це є офіційна документована можливість. Таким чином для приховування певних об’єктів достатньо реалізувати такий драйвер-фільтр та прикріпити його до кожного пристрою кожного логічного диску у системі. В самому драйвері достатньо перехоплювати пакети вводу/виводу, що відносяться до запиту вмісту директорі (IRP_MJ_DIRECTORY_CONTROL, IRP_MN_QUERY_DIRECTORY). Інформація повертається у вигляді зв’язаного списку, тож не має ніяких проблем, щоб модифікувати його в разі потреби (тобто видалити ті елементи списку, що необхідно приховати).

Переваги цього методу наступні:

- відсутня залежність від типу файлової системи;
- використання документованого методу вбудовування драйверу;
- централізований перехват функцій в одному місці (тобто немає потреби перехоплювати для кожного окремого процесу).

Недоліки методу:

- високі вимоги до кваліфікації фахівця.

Таким чином, враховуючи всі “за” та “проти” розглянутих вище методів, та на підставі практичних випробувань, найбільш прийнятним для приховування об’єктів файлової системи визнано четвертий метод, тобто приховування шляхом розробки драйвера-фільтра файлової системи. Перевагу цьому методу було надано ще й тому, що об’єкти, які треба приховувати, є результатом роботи програмного забезпечення системи спостереження за діяльністю користувача. Тобто, як сама система так і будь яке її проявлення повинні бути непомітними зовні, щоб виключити можливість знищення спостереження.

Література

1. Колисниченко Д. Н. Rootkits под Windows, Видавництво «Наука и техника» - Санки-Петербург, 2006. – 320 с.
2. Г. Хоглунд, Дж. Батлер Руткиты. Внедрение в ядро Windows, Видавництво «Addison-Wessley», «Питер» - СПб, 2007. – 285 с.