УДК 004.056.52

Гуцуляк Н. О.
Каплун В.А.

ВІДСТЕЖЕЖННЯ СИСТЕМНИХ ПОДІЙ ЗА ДОПОМОГОЮ ХУКІВ

Анотація. *Стаття описує основні методи відстеження системних подій, поняття програм-шпигунів, їх види та методи застосування. Розроблено два програмних модулі для стеження за подіями на комп'ютері, а саме: за екраном та клавіатурою, запропоновано встановлення даних програм як модулів, задля підвищення інформаційної безпеки.*

Ключові слова: *програми-шпигуни, модульні програми, інформаційна бехпека.*

Abstract. *The article describes the main methods of tracking system events, the concept of spyware, their types and methods of application. Two software modules have been developed to monitor events on the computer, namely: the screen and the keyboard, and it has been proposed to install these programs as modules in order to increase information security. spyware, modular software, information security.*

Keywords: *spyware, modular software, information security.*

Вступ

Багато сфер діяльності сучасного суспільства залежать від комп'ютерних технологій. У зв'язку з цим гостро постає питання конфіденційності інформації. Персональний комп'ютер став частиною нашого життя і тому надзвичайно важливим є питання стеження за діями, які відбуваються і даними які зберігаються на ньому.

У світі, де наші персональні дані, банківські рахунки, особиста інформація знаходяться в електронному вигляді є великий ризик не зберегти їх конфіденційність. Але так само є і потреба відслідковувати шахрайство, насильство та інші незаконні дії в мережі. Тому як знайти «золоту середину» і чиї дії можна і потрібно відслідковувати і чиї ні є доволі цікавим і актуальним питання на сьогоднішній день.

Метою роботи є дослідження методів сучасного стеження та створення модульних програм для стеження за системними подіями за допомогою хуків, а саме для захоплення клавіатури і монітору. Створені модулі нададуть змогу вирішити проблему захисту персональних даних в ті моменти коли вас немає поруч. Наразі, безпека інформації є не менш важливою, ніж сама інформація. А отже, для запобігання наданням доступу необхідно впроваджувати методи стежиння.

Результати дослідження

Програмні застосунки не мають наявного інтерфейсу, оскільки головною ідеєю програм-шпигунів є непомітність їх роботи. Для звичайного користувача вони абсолютно не помітні. Зовні нічого не відображається і на роботу за машиною не впливає.

Одразу після запуску, програмний модуль Keylogger починає перехоплювати події вводу даних з клавіатури. Після того, як будуть отримані перші дані, тобто буде натиснута клавіша, створиться два текстових файли keys.log та vk_keys.log. У файл keys.log записуються дані про кнопки, які не відносяться до літер та цифр, а саме backspace, shift, esc, tab, delete, alt, up, down та інші, а у файл vk_keys.log записуються віртуальні коди кнопок (англ. Virtual keys).

Після запуску засобу для відстеження екрану монітора – Screenlogger. Заданий алгоритм здійснює захоплення екрану по параметрам так, щоб знімок екрану в результаті був коректним. Завдяки цьому зміна монітору із більшим чим меншим розширенням не вплине на роботу застосунку. Навіть наявність другого підключеного монітору, як це часто буває не вплине ніяк чином. Після захоплення відбувається збереження зображення із вказаною датою та часом геть до секунд, дата та час записується у назву зображення.

Дані програмні модулі можуть використовуватися як самостійно, так і впроваджуватися в інші програми. Важливо зазначити, що тільки метод застосування (зокрема, апаратних або програмних продуктів, що включають кейлогер або скрінлогер як модуль) дозволяє побачити грань між управлінням безпекою та порушенням безпеки.

Приклади санкціонованого використання програм:

- визначити всі випадки набору на клавіатурі критичних слів і словосполучень, передача яких третім особам приведе до матеріального збитку;
- мати можливість дістати доступ до інформації, що зберігається на жорсткому диску комп'ютера, у разі втрати логіна і пароля доступу з будь-якої причини (хвороба співробітника, навмисні дії персоналу і так далі);
- визначити (локалізувати) всі випадки спроб перебору паролів доступу;
- проконтролювати можливість використання персональних комп'ютерів в неробочий час і виявити, що набиралося на клавіатурі в кожен конкретний момент;
- досліджувати комп'ютерні інциденти;
- проводити наукові дослідження, пов'язані з визначенням точності, оперативності і адекватності реагування персоналу на зовнішні дії;
- відновити критичну інформацію після збоїв комп'ютерних систем.

Приклади несанкціонованого використання програм:

- перехоплювати чужу інформацію, що набирається на клавіатурі;
- дістати несанкціонований доступ до логінів і паролів доступу в різні системи, включаючи системи типу «банк-клієнт»;
- дістати несанкціонований доступ до систем криптографічного захисту інформації користувача комп'ютера – парольних фраз;
- дістати несанкціонований доступ до авторизаційних даних кредиток.

Висновки

Досліджено методи стеження за системними подіями за допомогою хуків та шляхом використання програм-шпигунів. Наведено принцип роботи та використання хуків, висвітлено поняття програм-шпигунів, їх класифікацію, методи та сфери застосування.

Доведено актуальність і доцільність використання програм для стеження задля забезпечення конфіденційності інформації. Визначено межу законності використання програм для стеження за комп’ютером. Було розроблено програмні модулі для стеження за системними подіями. Реалізовано засіб перехоплення даних введених з клавіатури шляхом перехоплення системних подій з використанням хуків. Також реалізовано засіб для стеження за екраном монітора комп’ютера. Реалізовані застосунки класифікуються як програмні модулі для стеження і можуть бути використання як для впровадження у інші програми так і для самостійного функціонування.

Програмні модулі перевірено та доведено їх функціональну працездатність та відповідність поставленим задачам.

Отже, в рамках законів про конфіденційність особистої інформації дані програмні модулі можуть застосовуватися як програми-шпигуни для збору інформації або можуть бути націлені на відстеження помилок чи збоїв та здійснювати контроль за інформаційними системами виконуючи роль програм-моніторів.

Список використаної літератури

1. «Шпигунські програми» [Електронний ресурс]. Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/shpionskiye-programmy/.
2. «Закон про інформацію» [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
3. «Заметки Сис. Админа» [Електронний ресурс]. Режим доступу: https://sonikelf.ru/keylogger-chto-eto-ili-shpionazh-chistoj-vody-na-pk/
4. «Более эффективное использование C++»/ Скотт Майерс.

Гуцуляк Назарій Олегович – студент групи 1БС-18б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nazaripeople@gmail.com

Каплун Валентина Аполінаріївна, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

Hutsuliak Nazariy O.– Department of Information Technology and Computer Engineering , Vinnytsya National Technical University, Vinnytsia.

Valentyna A. Kaplun – Lecturer of the Chair of Safety of Infomation and Communication Systems, NTU, Vinnytsia.