УДК 004.056

Гуцуляк Н. О.
Лукічов В.В.

Засіб моніторингу користувацької активності. Розробка модуля моніторингу та аналізу

Вінницький національний технічний університет

Анотація. *Стаття описує основні методи моніторингу користувацької активності, поняття програм-шпигунів, їх види та методи застосування. Розроблено програмний засіб із режимом клієнт-сервер для стеження за процесами та характеристиками комп'ютера, а саме: за даними про апаратне забезпечення персонального комп'ютера, встановлене програмне забезпечення, документами відправленими на друк, за списком запущених процесів, підключених USB-носіїв, відкритих веб-сторінок, задля підвищення ефективності моніторингу додано можливість стеження за екраном та клавіатурою, запропоновано встановлення даних програми, задля підвищення інформаційної безпеки.*

Ключові слова: *моніторинг користувацької активності програми-шпигуни, інформаційна безпека.*

Abstract. *The article describes the main methods of monitoring the use of activities, the concept of spyware, their types and methods of application. Developed software with client-server mode for monitoring the processes and characteristics of the computer, namely: data on personal computer hardware, installed software, documents sent to print, the list of running processes, connected USB media , open web pages, to improve the effectiveness of monitoring added the ability to monitor the screen and keyboard, recommended data installation to improve information security.*

Keywords: *monitoring user activity, pyware, 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[1].

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, а чиї ні, є доволі цікавим і актуальним питання на сьогоднішній день[2].

Метою роботи є дослідження методів сучасного стеження та створення універсального дистанційного моніторингового застосунку для стеження за системними процесами та даними для подальшого аналізу. Створений програмний застосунок надасть 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 стеження[3].

Результати дослідження

Програмний застосунок має зручний і зрозумілий інтерфейс, засіб дає змогу працювати у різних режим, а саме збирати потрібні для аналізу дані з комп'ютера. Усі зібрані дані відправляються на сервер, з якого ведеться моніторинг.

Одразу після запуску клієнтської сторони застосунку, встановлюється з'єднання зі сервером, після чого з'являється можливість вибрати режим роботи моніторингового засобу, а саме обрати вид інформації, яку потрібно відстежити[4]. Серед доступних видів інформації що можна відстежити, є наступні:

- дані про апаратне забезпечення персонального комп'ютера;
- дані про встановлене програмне забезпечення;
- список запущених процесів;

- список підключених USB-носіїв;
- дані про документи відправлені на друк;
- дані про відкриті веб-сторінки.

Також серед доступних можливостей засобу для моніторингу користувацької діяльності є програмний модуль Keylogger, який активується після натискання відповідної кнопки. Модуль 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, що активується натисканням аналогічної кнопки. 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 програмний застосунок використовуватися як самостійно, серверна частина встановлюється окремо від клієнтської. Важливо зазначити, що тільки метод застосування (зокрема апаратних або програмних продуктів, що включають засоби моніторингу) 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[5]:

- перехоплювати чужу інформацію;
- 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

Було досліджено методи моніторингу користувацької діяльності. Наведено принцип роботи та використання різних підходів стеження, висвітлено поняття програм-шпигунів, їх класифікацію, методи та сфери застосування[6].

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 про встановлене програмне та апаратне забезпечення, процеси та події на комп’ютері, введених з клавіатури символів. Також реалізовано засіб для стеження за екраном монітора комп’ютера. Реалізований застосунок працює самостійно в режимі клієнт-сервер.

Програмний засіб перевірено та доведено їх функціональну працездатність та відповідність поставленим задачам.

Отже, в рамках законів про конфіденційність особистої інформації даний засіб моніторингу користувацької діяльності може застосовуватися як програма-шпигун для збору інформації або може бути націлений на відстеження помилок чи збоїв та здійснювати контроль за інформаційними системами виконуючи роль програми-моніторингу.

Список використаної літератури

1. Бобал Ю. Я. Горбатий І. В. Інформаційна безпека. Львівська політехніка. 2019. 580 с.
2. Закон України про інформацію, Закон від 02.10.1992 № 2657-XII. Київ (Редакція станом на 01.01.2022) 650с.
3. Кудін Д. Д. Спостережуваність обчислювальних систем як невід'ємна частина комплексу засобів захисту в автоматизованій системі. http://bezpeka.com/ru/lib/spec/infsys/art119.html
4. Едвард Сноуден Особова справа. КМ-БУКС. Київ 2020, 336 с.
5. Джозеф Менн Культ мертвої корови. Фабула. Харків 2021, 240 с.
6. William Sutcliffe We See Everything. Bloomsbury. 2018, 272 p.

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

Лукічов Віталій Володимирович — кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет , м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Nazarii Hutsuliak – Department of Information Technology and Computer Engineering , Vinnytsya National Technical University, Vinnytsia, e-mail: nazaripeople@gmail.com..

Vitaliy Lukichov – PhD (Eng), Senior Lecturer of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua.