Список використаних джерел:

1. Організація баз даних : навч. посібник / О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, І. М. Копитчук. 2-ге вид. виправ. і доповн. Одеса : Фенікс, 2019. С. 7-8.
2. Hassan Bediar. Challenges and Security Vulnerabilities to Impact on Database Systems. *Al-Mustansiriyah Journal of Science*. Volume 29, Issue 2, 2018. DOI: http://doi.org/10.23851/mjs.v29i2.332. URL: https://www.researchgate.net/publication/329025438_Challenges_and_Security_Vulnerabilities_to_Impact_on_Database_Systems
3. Логінова Н. І. Безпека баз даних. *Кібербезпека в сучасному світі* : матеріали ІІІ Всеукр. наук.-практич. конф. (м. Одеса, 19 листоп., 2021 р.) / за ред. О. В. Дикого; уклад.: С. А. Горбаченко, Н. І. Логінова. Одеса : Видавничий дім «Гельветика», 2021. С. 12–15. DOI 10.32837/11300.15973.
4. TOPDB Top Database index. URL: https://pypl.github.io/DB.html

Ключові слова: бази даних, системи керування базами даних, вразливості, безпека, загрози, ризики.

Key words: databases, database management systems, vulnerabilities, security, threats, risks.

ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

КУХАРЕНКО СЕРГІЙ ВІКТОРОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ВИТОКІВ В ОПЕРАЦІЙНИХ СИСТЕМАХ СІМЕЙСТВА WINDOWS

Більшість користувачів операційної системи (ОС) Windows зустрічали у списку диспетчера завдань, безліч процесів з ім'ям *svchost.exe*. Залежно від версії ОС Windows та її конфігурації, кількість таких процесів може становити від кількох одиниць до кількох десятків.

Це пояснюється тим, що *svchost.exe* є основним процесом для системних служб ОС Windows, що завантажуються з динамічних бібліотек (*.dll). Виконуваний файл *svchost.exe* розміщено у системному каталозі \Windows\system32\. Запуск системних служб організований так, що дозволяє суттєво зменшити витрати оперативної пам'яті та ресурсів процесора. Усі копії процесів ***svchost.exe*** запускаються системним процесом *services.exe* під час початкового завантаження ОС Windows, а також під час виконання системних процесів та процесів, пов'язаних

із запуском прикладного програмного забезпечення (ППЗ) користувача [1].

Системні процеси ОС Windows, особливо ті, за запуск яких відповідає процес *svchost.exe*, є необхідними компонентами для її повноцінної роботи [2]. У процесі завантаження ОС Windows здійснюється запуск служб:

- диспетчер мережевих підключень;
- планувальника завдань;
- Plug and Play та HID;
- центр оновлення;
- захисника ОС Windows;
- фонової інтелектуальної служби передачі BITS та інших.

При запуску ОС Windows служба *svchost.exe* перевіряє розділи реєстру зі службами та створює список служб, які завантажуються в оперативну пам'ять. Кожен сеанс служби *svchost.exe* може виконуватися у вигляді групування служб. Така організація необхідна для зменшення кількості різних запущених служб та покращує їх можливе налагодження, якщо в цьому буде потреба. Наприклад, один процес *svchost.exe* запускає декілька служб, пов'язаних із вбудованим мережевим екраном ОС Windows [3], який за замовчанням безперешкодно пропускає всі його вихідні з'єднання за наявності підключення до цифрового простору Інтернет (рис. 1).

Рис. 1. Схема організації з'єднань служби *svchost.exe* з цифровим простором Інтернет

Такі налаштування вбудованого мережевого екрану є заздалегідь встановленими в ОС Windows на комп'ютер користувача. Ця обставина, у свою чергу, призводить до повного або часткового дублювання всіх вихідних/вхідних з'єднань, що здійснюються прикладним програмним забезпеченням (ППЗ) користувача, що само по собі є потенційною загрозою для витоків персоналізованих даних користувача (рис. 2).

Для здійснення регламентованого доступу до цифрового простору Інтернет у сімействі ОС Windows передбачено наявність вбудованого брандмауера (мережевого екрану) – системного програмного забезпечення, яке виконує контроль за обміном даними між ОС Windows та цифровим простором Інтернет [4].

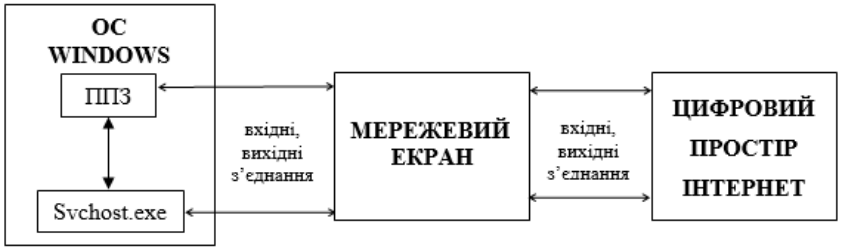

Рис. 2. Організація обміну даними між ОС Windows, ППЗ та цифровим простором Інтернет

Однак, як показує довготривала практика поглибленого дослідження мережевого трафіку ОС Windows, ППЗ та мережевого процесу *svchost.exe* з цифровим простором Інтернет із застосуванням сніферів [5] – вбудований мережевий екран безперешкодно пропускає більшість вихідних/вхідних з'єднань системного ПЗ ОС Windows та ППЗ, які неминуче призводять до витоків персональних даних користувача [6; 7].

Аналіз трафіку вихідних/вхідних з'єднань дозволив поділити їх на робочі та сторонні. Також у процесі поглибленого аналізу було встановлено наявність вихідних з'єднань мережного процесу *svchost.exe*, які можна класифікувати, як сторонні, оскільки вони ініціюються ППЗ і здебільшого не відповідають вихідним з'єднанням самого ППЗ (рис. 3).

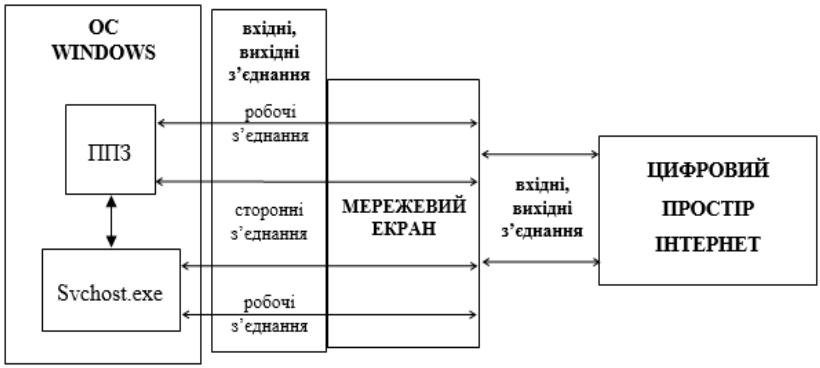

Рис. 3. Взаємозв'язок сторонніх і робочих з'єднань ОС Windows, ППЗ і цифровим простором Інтернет

Така організація вихідних/вхідних з'єднань у ОС Windows може з високою ймовірністю призвести до витоку персональних даних користувачів. Для усунення цієї проблеми необхідно примусове блокування сторонніх з'єднань ППЗ та мережевого процесу *svchost.exe* (рис. 4).

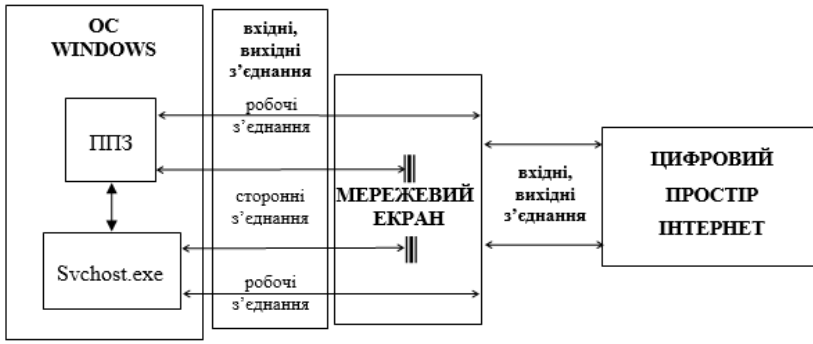

Рис. 4. Організація блокування сторонніх з'єднань ОС Windows та ППЗ з цифровим простором Інтернет

У процесі тривалого моніторингу та подальшого аналізу вихідних/вхідних з'єднань, при організації блокування сторонніх з'єднань ОС Windows та ППЗ (див. рис. 4), була експериментально підтверджена ефективність запропонованого підходу для організації захисту персональних даних від потенційно можливих витоків.

Список використаних джерел:

1. What Is the Service Host Process (svchost.exe) and Why Are So Many Running? URL: https://www.howtogeek.com/howto/windows-vista/what-is-svchostexe-and-why-is-it-running/. (Дата звернення 06.06.2022).
2. What is svchost.exe? 5 ways to see if it's safe. URL: https://www.glasswire.com/process/svchost.exe.html. (Дата звернення 06.06.2022).
3. Fix svchost.exe (netsvcs) High CPU Usage or Memory Leak Issue. URL: https://whatsabyte.com/svchost-exe-netsvcs-high-cpu/ (Дата звернення 06.06.2022).
4. Naik N. and Jenkins P. «Enhancing Windows Firewall Security Using Fuzzy Reasoning,» 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2016, pp. 263–269, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.64.
5. Bo Yu, «Based on the network sniffer implement network monitoring,» 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010, pp. V7-1-V7-3, doi: 10.1109/ICCASM.2010.5620505
6. Algorithm of user's personal data protection against data leaks in Windows 10 OS / Olexander V. Zadereyko, Olena G. Trofymenko, Nataliia I. Loginova //

Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, vol. 9, p. 41–44. URL: https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-b9e2407a-7fc7-41bf-a947-c285ad6b6d70
7. Zadereyko A. Development of algorithm to protect user communication devices against data leaks / A. Zadereyko, Y. Prokop, O. Trofymenko, N. Loginova, O. Plachinda // Eastern-European Journal of Enterprise Technologies. – V. 1/2 (109) – Technology Center, 2021. – P. 24–34. URL: http://dspace.onua.edu.ua/handle/11300/14489

Ключові слова: витоки персональних даних, витоки даних в ОС Windows, блокування витоків персональних даних.
Key words: personal data leaks, data leaks in Windows OS, blocking of personal data leaks.

ЛОБОДА ЮЛІЯ ГЕННАДІЇВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

СУЧАСНІ ІНСТРУМЕНТИ АНАЛІЗУ ДАНИХ ЗА ДОПОМОГОЮ GOOGLE ANALYTICS

Сучасні інструменти веб-аналітики пропонують безліч привабливих функцій та переваг від керівників вищої ланки та до фахівців з реклами та маркетингу, від власників сайтів та до розробників контенту. Вони дозволяють відстежувати продуктивність програм, поведінку користувачів на сайті, вимірювати трафік та багато іншого. Наприклад, Google Analytics використовують приблизно 28,8 млн активних веб-сайтів, що становить близько 85,9 % ринку веб-аналітики [1].

Так, Google Analytics використовує новий тип ресурсу Google Analytics 4, який дозволить аналізувати всі необхідні дані в єдиному інтерфейсі для того, щоб було простіше приймати рішення, аргументуючи це такими причинами:

1. Масштабована кроссплатформова аналітика, яка будується навколо подій (events).
2. У новому ресурсі всім користувачам Google Analytics доступні машинне навчання (machine learning, ML) та функції NLP.
3. У пріоритеті збереження конфіденційності, у тому числі позбавлення необхідності встановлювати cookies.
4. Безшовна інтеграція з усіма продуктами Google.
5. Міжплатформна ідентифікація користувачів. У новому ресурсі можна побачити весь шлях користувача, тобто всі його дії на різних девайсах та платформах.

Розгляньмо ці переваги докладніше.