УДК 004.056.5:004.491.4

В. О. Лагодзінський
Є. В. Радченко

АНАЛІЗ НАЯВНИХ ЗАСОБІВ ЗАХИСТУ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОС LINUX

Вінницький національний технічний університет, м. Вінниця

Анотація

У роботі проведено аналіз наявних засобів захисту від шкідливого програмного забезпечення для операційної системи Linux. Розглянуто основні категорії антивірусного програмного забезпечення, систем виявлення вторгнень та інструментів моніторингу цілісності файлів.

Ключові слова: Linux; шкідливе програмне забезпечення; антивірус; захист інформації; кібербезпека; IDS; моніторинг цілісності.

Abstract

The paper analyzes the existing means of protection against malware for the Linux operating system. The main categories of antivirus software, intrusion detection systems and file integrity monitoring tools are considered. It was found that the functional capabilities of existing Linux security solutions are significantly inferior to similar products for Windows, which necessitates increased development of specialized software for this platform.

Keywords: Linux; malware; antivirus; information security; cybersecurity; IDS; integrity monitoring.

Вступ

Операційна система Linux займає провідні позиції у серверній інфраструктурі, хмарних середовищах та вбудованих системах. За даними компанії Red Hat, понад 90% публічних хмарних робочих навантажень функціонують під управлінням Linux-систем [1]. Разом з тим, зростання популярності платформи супроводжується збільшенням кількості кіберзагроз, спрямованих саме на Linux-середовища. Зокрема, дослідження компанії CrowdStrike зафіксувало зростання кількості шкідливого програмного забезпечення для Linux на 35% у 2022 році порівняно з попереднім роком [2]. Це актуалізує питання ефективності та достатності наявних засобів захисту для даної платформи.

Постановка проблеми

Незважаючи на поширеність Linux у критичній інфраструктурі, ринок засобів кібербезпеки для цієї платформи залишається суттєво менш розвиненим порівняно з екосистемою захисту Windows. Більшість комерційних антивірусних продуктів зосереджені на виявленні загроз для Windows-середовища, тоді як специфічні Linux-загрози (руткіти, криптомайнери, бекдори) нерідко залишаються поза зоною охоплення. У даній роботі ставиться завдання систематизувати наявні інструменти захисту від шкідливого програмного забезпечення для Linux та визначити напрями їх подальшого розвитку.

Основні результати

На основі проведеного аналізу виокремлено три основні категорії засобів захисту від шкідливого програмного забезпечення для Linux:

- **Антивірусне програмне забезпечення:** найбільш поширеними рішеннями є ClamAV (відкрите ПЗ), Kaspersky Endpoint Security for Linux, ESET NOD32 Antivirus for Linux та Dr.Web для Linux. ClamAV — відкритий антивірусний рушій, орієнтований на пакетне сканування файлів і поштових повідомлень без вбудованого захисту у реальному часі [4]. Комерційні рішення пропонують більш широкий функціонал, однак їх вартість та ресурсомісткість обмежують застосування у вбудованих системах.
- **Системи виявлення вторгнень (IDS/IPS):** до ключових інструментів належать OSSEC (HIDS із відкритим кодом), Suricata та Snort (мережеві IDS), а також Wazuh — платформа на базі OSSEC із розширеними можливостями. Wazuh забезпечує централізований моніторинг подій безпеки, інтеграцію з SIEM-системами та підтримку стандартів відповідності PCI DSS і GDPR [5]. Проте налаштування та підтримка зазначених систем вимагають глибоких технічних знань, що ускладнює їх впровадження у невеликих організаціях.
- **Засоби моніторингу цілісності файлів та аудиту системи:** AIDE (Advanced Intrusion Detection Environment) та Tripwire здійснюють контроль змін у файловій системі шляхом порівняння хеш-

сум. Фреймворк auditd, вбудований у ядро Linux, дозволяє відстежувати системні виклики та доступ до файлів. Lynis є інструментом аудиту безпеки та оцінки відповідності конфігурацій системи [5]. Разом з тим, ці інструменти є реактивними за своєю природою і не запобігають зараженню, а лише фіксують його факт.

Порівняльний аналіз наявних рішень свідчить про суттєву асиметрію між екосистемами безпеки Windows та Linux. Для Windows характерна наявність зрілих комплексних EDR-платформ (Microsoft Defender for Endpoint, CrowdStrike Falcon, SentinelOne), які поєднують антивірусний захист, поведінковий аналіз, автоматичне реагування та інтеграцію з хмарними сервісами кіберрозвідки. Аналогічні повнофункціональні рішення для Linux або відсутні, або є портами Windows-продуктів із обмеженою функціональністю. Зокрема, більшість Linux-орієнтованих EDR не підтримують автоматичне усунення загроз, а покриття виявлення Linux-специфічних руткітів залишається на рівні 60–70% від Windows-аналогів [2].

Висновки

Проведений аналіз підтверджує, що наявні засоби захисту від шкідливого програмного забезпечення для Linux охоплюють базові потреби у сфері безпеки, однак за функціональним наповненням значно поступаються рішенням для Windows. Фрагментованість інструментарію, висока складність налаштування та відсутність зрілих комплексних EDR-платформ є системними проблемами безпеки Linux-середовища. З огляду на зростаючу роль Linux у критичній інфраструктурі, державних системах та хмарних обчисленнях, дана тематика зберігатиме свою актуальність у довгостроковій перспективі. Подальші дослідження та розробки доцільно спрямувати на створення нативних Linux EDR-рішень із підтримкою поведінкового аналізу, автоматичного реагування та машинного навчання для виявлення невідомих загроз. Активізація розробки спеціалізованого програмного забезпечення для Linux є необхідною умовою забезпечення належного рівня кібербезпеки сучасної цифрової інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Linux Foundation. Linux Kernel Development: How Fast It Is Going, Who Is Doing It, What They Are Doing, and Who Is Sponsoring It. The Linux Foundation, 2020. URL: https://www.linuxfoundation.org/resources/publications/linux-kernel-report-2020 .
2. CrowdStrike. 2023 Global Threat Report. CrowdStrike Inc., 2023. URL: https://www.crowdstrike.com/global-threat-report/ .
3. National Vulnerability Database (NVD). NIST. URL: https://nvd.nist.gov .
4. ClamAV Documentation. Cisco Systems, Inc., 2024. URL: https://docs.clamav.net/Introduction.html.
5. Wazuh Documentation. Wazuh Inc., 2024. URL: https://documentation.wazuh.com.

Лагодзінський Вадим Олегович – студент групи 2БС-25Б, факультет інформаційних технологій та комп'ютерної інженерії. Вінницький національний технічний університет, Вінниця, email: Vadimlagod1@gmail.com

Науковий керівник: Радченко Євген Валентинович – асистент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця Email: eradchenko@vntu.edu.ua

Lagodzinskyi Vadym Olehovych – student of group 2BS-25B, Faculty of Information Technology and Computer Engineering. Vinnytsia National Technical University, Vinnytsia, email: Vadimlagod1@gmail.com

Scientific Advisor: Radchenko Yevhen Valentynovych – Assistant at the Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia. Email: eradchenko@vntu.edu.ua