Дослідження журналів подій операційних систем macOS в цифровій криміналістиці

Євген Панов

головний судовий експерт, Сумський НДЕКЦ МВС України, м. Суми, Україна,
e-mail: exp.peo@gmail.com

Розглянуто основні типи журналів macOS, важливі аспекти в криміналістиці на macOS; команди та інструменти для роботи з журналами, зокрема команда log; інструменти для аналізу.

Ключові слова: *журнали подій; macOS; команда log.*

Investigation of MacOS Event Logs in Digital Forensics

Yevhen Panov

Principal types of macOS logs, important aspects in macOS forensics, commands and tools for working with logs, particularly the log command, and tools for analysis are considered.

Keywords: *event logs; macOS; log command.*

macOS — це серія операційних систем, розроблених компанією Apple для комп'ютерів Mac. Вона побудована на базі ядра Unix і є однією з найпопулярніших операційних систем для настільних комп'ютерів та ноутбуків. macOS вирізняється високим рівнем безпеки, стабільності та інтеграції з іншими продуктами Apple.

Дослідження журналів подій операційної системи macOS є важливою складовою цифрової криміналістики, оскільки журнали містять докладні відомості про активність користувачів і системних процесів, що допомагає в розслідуванні інцидентів. У випадках зламу, несанкціонованого доступу або інших кібератак журнали подій можуть бути ключовим джерелом інформації для відновлення послідовності подій і виявлення слідів зловмисників.

Основні типи журналів в macOS

1. *Журнал системних подій (system.log)* зберігає загальну інформацію про події в системі, зокрема, системні помилки, повідомлення про завантаження програм та інші події, які можуть бути корисними для виявлення проблем або підозрілої активності. Розташування: /var/log/system.log.

2. *Журнали безпеки та автентифікації (/var/log/asl.log, authd.log)* відстежують спроби входу в систему, зміну прав доступу, помилки автентифікації, що є важливим для розслідування несанкціонованого доступу. Розташування: /var/log/authd.log, /var/log/asl/.

3. *Unified Logging System (ULS)* запроваджений у macOS 10.12 Sierra. Це сучасна система ведення журналів, яка забезпечує централізоване збирання та зберігання всіх журналів у єдиному форматі. Інструмент для доступу: log команда, яка дає змогу виконувати пошук і фільтрацію подій через термінал.

Команда log для роботи з журналами

Основний інструмент для роботи з ULS — це команда log. Вона дає змогу:

- переглядати журнали в реальному часі: log stream. Застосовується для спостереження за поточною активністю в системі;
- шукати події за певними критеріями: log show --predicate 'eventMessage contains «error»' – info. Ця команда фільтрує події, які містять слово «error».

- виконувати пошук подійз а часовим проміжком, що особливо корисно для криміналістичних розслідувань: log show --start '2024-01-01 00:00:00' --end '2024-01-01 23:59:59'.

Інструменти для аналізу

1. *Syslog* — класичний інструмент для роботи з журналами системи. Допомагає виводити та фільтрувати події. Приклад для виведення помилок: cat /var/log/system.log | grep «error».

2. *Consolation* — графічний інтерфейс для аналізу журналів macOS, що працює з Unified Logging System і надає зручний інтерфейс для пошуку та аналізу подій.

3. *ELK Stack (Elasticsearch, Logstash, Kibana)* — потужний набір інструментів для збирання, індексації та візуалізації даних із журналів. Застосовується для централізованого збирання логів із декількох систем і візуалізації даних для аналізування тенденцій.

Процес криміналістичного аналізу

1. Збирання доказів

Збирання всіх відповідних журналів із системи є першим кроком у розслідуванні. Важливо зберегти журнали в первинному вигляді, аби не порушити докази. Для збереження всіх журналів застосовується інструмент log collect: log collect --output /path/to/save/logarchive.

2. Хронологічний аналіз

Аналізуються часові позначки подій для відновлення точної послідовності дій. Це допомагає визначити, коли зловмисник увійшов до системи, які дії він виконував і чи була компрометація інших облікових записів.

3. Ідентифікація підозрілої активності

Перевіряються всі журнали на предмет незвичної активності: запуск незвичних процесів, спроби підвищити привілеї, зміна конфігураційних файлів або неочікувані мережеві з'єднання.

4. Аналізування автентифікації та безпеки

Перевіряються журнали автентифікації, щоб виявити можливі спроби зламу облікових записів: невдалі спроби входу, зміну паролів або створення нових облікових записів.

Важливі аспекти в криміналістиці на macOS

1. Незмінність доказів. Важливо працювати з копіями журналів, щоб зберегти оригінали незміненими, тому що будь-яка зміна може знищити докази або ускладнити застосування їх в суді.

2. Часові зони та синхронізація. Під час аналізування подій слід звертати увагу на часові пояси й коректність синхронізації часу між системами.

3. Зловмисні процеси. Не завжди зловмисні дії відображаються як помилки або відмови. Потрібно звертати увагу на маловідомі або підозрілі процеси, які могли бути запущені в результаті атаки.

Журнали подій macOS є критично важливим джерелом інформації в цифровій криміналістиці. Вони допомагають відновити хронологію подій, ідентифікувати зловмисні дії та зібрати докази, необхідні для розслідування кіберзлочинів.

Перелік джерел посилання

1. «The Art of Mac Malware» — Patrick Wardle.
2. «OS X Incident Response: Scripting and Analysis» — Jaron Bradley, Jesse Varsalone.
3. «Practical Forensic Imaging: Securing Digital Evidence with Linux Tools» — Bruce Nikkel.
4. «Digital Forensics with Open Source Tools» — Cory Altheide, Harlan Carvey.