МЕХАНІЗМИ ПРОВЕДЕННЯ ЦИФРОВОЇ КРИМІНАЛІСТИЧНОЇ ЕКСПЕРТИЗИ ЕЛЕКТРОННОЇ ПОШТИ

Снігуров А.В., Василина Ю.В.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: arkadii.snihurov@nure.ua,
yuliia.vasylyna@nure.ua

Abstract

The report analyzes the possibilities of conducting a digital forensic examination of e-mail. The relevance of this topic lies in the massive use of e-mail by criminals to carry out cyber-attacks (sending malicious programs, spam, phishing), carrying out other criminal actions, such as blackmail, messages about landmines, etc. The report analyzes the peculiarities of e-mail construction, methods and means of conducting digital forensic examination of e-mail, problems of identifying criminals during digital forensic examination of e-mail.

Питанням розробки механізмів проведення криміналістичної цифрової експертизи присвячено багато публікацій, в тому числі [1,2,3,4]. Одним з напрямків проведення досліджень в цій сфері є механізми цифрової експертизи електронної пошти. Електронна пошта на даний час є одним з основних інструментів комунікації разом з мобільним зв'язком, месенджерами, соціальними мережами. Здебільшого електрона пошта зараз використовується у сфері професійної комунікації. Організації, посадові особи, співробітники мають електронні адреси, які можуть бути офіційно опубліковані. Створити електронну адресу зараз дуже легко і займає кілька хвилин. Існує значна кількість поштових сервісів, таких як Gmail, Yahoo, Hotmail, Outlook, macOS Mail, Mailbox, ProtonMail та інші. Дана ситуація призводить не тільки до збільшення можливості комунікації, а й виникненню великої кількості кіберзагроз, які реалізуються через електронну пошту. Розсилка шкідливих програм, спаму, загроз фізичної розправи, загроз про замінування організації, шантаж тощо. В цих умовах важливим завданням в сфері інформаційної безпеки є розробка механізмів проведення цифрової криміналістичної експертизи електронної пошти. Це достатньо важка сфера цифрової криміналістики, в якій не завжди можливо отримати бажаний результат. Метою доповіді є аналіз механізмів побудови сервісів електронної пошти, аналіз можливостей отримання інформації про зловмисника шляхом аналізу артефактів електронної пошти.

На даний час поштові клієнти поділяються на два типи за місцем зберігання електронних повідомлень: Web-based клієнти електронної пошти - зберігають усі свої дані на веб-сервері (наприклад, Gmail, Yahoo Mail, Hotmail тощо), Desktop-based поштові клієнти - усі дані веб-браузера на настільному комп'ютері зберігаються в системі його користувачів (Outlook, Thunderbird, Mail Bird тощо).

Структура електронної пошти складається з різних елементів, таких, як поштові агенти користувача (Mail User Agent - MUA), агенти передачі пошти (Mail Transfer Agent - MTA), агенти з доставки пошти (Mail Delivery Agent - MDA), агенти пошуку пошти (mail retrieval agent - MRA) та інші. Протоколи, що використовуються – SMTP, POP, IMAP.

Під час проходження повідомлення від відправника до одержувача залишаються такі основні сліди:

- копія повідомлення в MUA відправника;
- запис у журналі кожного MTA, через який пройшло повідомлення (при проходженні через MTA копія повідомлення не зберігається, але в журналі робиться запис про його надходження та відправлення);
- копія повідомлення в MUA одержувача з доданими заголовками;

- траси, утворені в результаті доступу всіх MTA, через які пройшло повідомлення, до відповідних DNS-серверів як під час отримання, так і під час передачі повідомлення;

- записи в журналах антивірусних програм на всіх MTA, через які пройшло повідомлення, а також на комп'ютерах відправника та одержувача;

- сліди в журналах провайдерів, через які здійснювався зв'язок між MUA відправника та MTA відправника та між MUA одержувача та MDA / MTA одержувача.

Можливості виявлення підозрюваного в злочині, при використанні ним електронної пошти, дуже сильно залежать від можливості доступу експерта-криміналіста або поліції до усіх елементів системи електронної пошти. Якщо дуже стисло представити систему електронної пошти, як показано на рис. 1, то можна виділити основні можливості по аналізу.

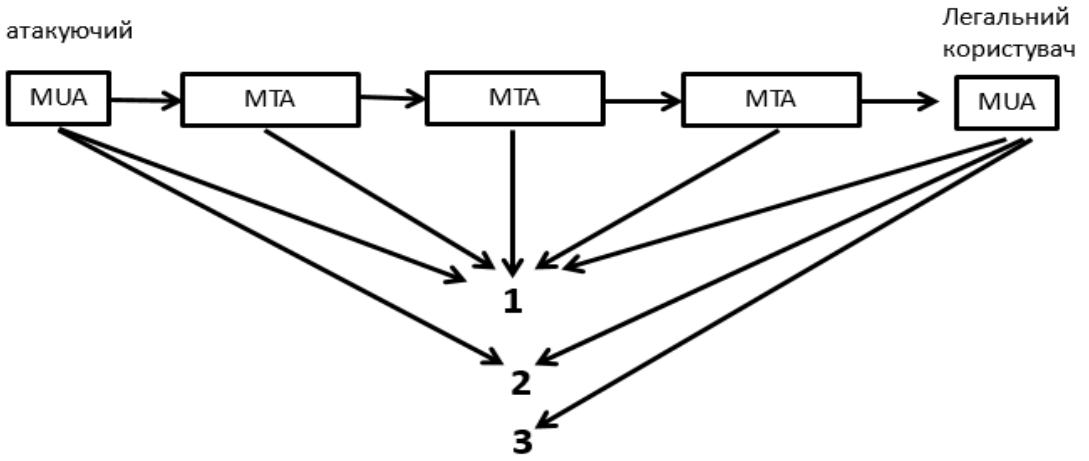

Рис. 1. Спрощена структура електронної пошти з поясненням ситуацій доступу експертів-криміналістів до її елементів

Ситуація 1. Експерт-криміналіст має доступ до комп'ютера атакуючого (підозрюваного в злочині) та легального користувача, а також до усіх проміжних серверів системи електронної пошти. При цьому є можливість аналізувати як повідомлення на кінцевих пунктах та знайти певні докази, а також можна аналізувати журнали проміжних серверів.

Ситуація 2. Експерт-криміналіст має доступ до комп'ютера легального користувача та комп'ютера атакуючого (підозрюваного в злочині). Атакуючий може стерти повідомлення.

Ситуація 3. Експерт-криміналіст має доступ тільки до комп'ютера жертви і може аналізувати тільки кінцеве повідомлення. На жаль, для нашої країни актуальний в значній кількості випадків варіант 3.

Під час аналізу повідомлення електронної пошти аналізується його заголовок та зміст. При аналізі змісту можна зрозуміти: чого хоче зловмисник: це фішинг, шантаж, шкідливий код, повідомлення про терористичні напади, залякування, спам, соціальна інженерія, листування злочинців (будь-який вид злочину). При аналізі заголовка, по-перше, необхідно зрозуміти, звідки прийшло повідомлення. При аналізі позиції "Received" визначаються IP-адреси усіх проміжних пунктів шляху переміщення повідомлення. При цьому можна використовувати існуючі інструменти аналізу e-mail заголовків, таких, наприклад, як https://toolbox.googleapps.com/apps/messageheader/analyzeheader. При аналізі заголовків вручну необхідно брати за увагу, що IP-адреса останнього вузлу на маршруті повідомлення знаходиться внизу, а першого вверху. Крім того при аналізі заголовків в деяких випадках можна знайти інформацію про тип антивірусної програми на комп'ютері відправника повідомлення, ім'я його комп'ютера, тип поштового клієнта тощо.

Таким чином, виявлення підозрюваного в скоєнні протиправних дій, при використанні їм електронної пошти, є непростим завданням, результат якого залежить від того, які клієнти електронної пошти він використовує, чи застосовує він заходи анти-форензики тощо. На даний час є необхідність створення методики аналізу електронної пошти для застосування її в правоохоронній дільності.

*Л*ітература

1. *Снігуров А.В., Балашов В.Ю., Сердюк А.Ю.* Аналіз механізмів реалізації мережевих атак прикладного рівня в інтересах проведення криміналістичних розслідувань кіберзлочинів / А. В. Снігуров, В. Ю. Балашов, А. Ю. Сердюк // Збірник наукових праць Харківського університету Повітряних Сил. - 2017. - № 2. - С. 64-68.

2. *Snihurov A., Shulhin O., Balashov V.* Experimental Studies of Ransomware for Developing Cybersecurity Measures // Proceedings of International Scientific-Practical Conference on Problems of Infocommunications Science and Technology. PIC S and T 2018, Kharkiv. - 2018. - P. 691-695.

3. *Снігуров А.В., Сірий М.С.* Методика проведення цифрової експертизи енергозалежної пам'яті комп'ютерів в інтересах розслідування кіберзлочинів. Інформатика, управління та штучний інтелект. Тези восьмої міжнародної науково-технічної конференції. Харків: НТУ "ХПІ". - 2021. - С. 128.

4. *Снігуров А.В., Сірий М.С.* Підхід до проведення цифрової експертизи оперативної пам'яті комп'ютерів в інтересах розслідування кіберзлочинів. Інформатика, управління та штучний інтелект. Тези восьмої міжнародної науково-технічної конференції. Харків: НТУ "ХПІ". - 2021. - С. 129.