УДК 343.1+004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7848-6448;
Олена Русланівна ЛЕЙКО,
студент факультету № 6
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ ЕЛЕКТРОННОЇ ПОШТИ

Із стрімким розвитком інформаційних технологій зростає кількість злочинів, як скоєних в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, так і загально кримінальних злочинів, в яких використовуються наявні сервіси глобальної комп'ютерної мережі [1,2].

Одним із сервісів глобальної мережі, який достатньо часто використовується злочинцями, є електронна пошта. Можна зазначити наступні способи зловмисного використання сервісу електронної пошти.

1. Масова розсилка електронних листів (спам). Має за мету розсилку комерційної та іншої реклами або листів із прикріпленими шкідливими програмами (інформації) особам, які не виражали бажання їх отримувати. Адреси електронник скриньок збираються пошуковими сервісами або отримуються із вкрадених баз даних персональної інформації.

2. Перешкоджання роботі поштової скриньки або серверу (поштова «бомба»). Здійснюється шляхом відправлення величезного обсягу даних на електронну адресу для того, щоб переповнити поштову скриньку або перевантажити поштовий сервер, і як результат порушити доступність скриньки або серверу.

3. Розповсюдження адрес підроблених веб-сайтів (фішинг). Має за мету переконати отримувача електронного листа перейти за певним посиланням на підроблений сайт, який імітує веб-сторінки існуючих корисних ресурсів і де необхідно вводити персональні дані автентифікації, які будуть після вводу вкрадені. Фішингові атаки можуть проводитись шляхом масової або цільової розсилки.

4. Підміна адреси відправника електронного листа (email spoofing). При зловмисному використанні електронної пошти підробляється адреса відправника електронного листа. Як правило, таку підміну використовують для розсилки спаму, фішинг-листів і шкідливих програм, щоб ввести одержувача в оману щодо походження листа.

При вчиненні загально кримінальних злочинів електронну пошту, як правило, використовують для:

1) зв'язку із потенційними жертвами з метою:

– шантажу;

– вимагання;

– погроз;

2) спілкування із співучасниками злочину.

Таким чином, при розслідуванні відповідних злочинів електронні поштові скриньки та електронні листи є об'єктами криміналістичного дослідження з метою виявлення і фіксації інформації в електронній (цифровій) формі, що містить дані щодо обставин вчинення кримінального правопорушення.

При криміналістичному аналізі електронної поштової скриньки необхідний фізичний доступ до поштового серверу і комп'ютеру підозрюваного для отримання логічної або побітової копії скриньки. Для виконання побітової копії скриньки використовуються спеціальні програмні засоби.

При криміналістичному аналізі електронних листів різними способами проводиться огляд службових заголовків електронного листа. Заголовки електронного листа містять достатньо суттєву, з точки зору кримінального розслідування, інформацію:

– час відправленого повідомлення;

– унікальні ідентифікаційні дані;

– IP-адресу сервера-відправника;

– зворотну адресу електронного листа;

– IP-адресу хосту з якого отримано листа;

– доменне ім'я комп'ютера, який приймав листа;

– дату передавання листа;

– час, коли одержано листа;

– тему листа;

– дата і час створення листа;

– відомості про поштову програму, яку використовували при відправці листа.

Аналіз заголовків можна здійснювати вручну, або за допомогою існуючих онлайн сервісів, наприклад таких:

– https://toolbox.googleapps.com/apps/messageheader/;

– http://ua.smart-ip.net/trace-email.

При наявності тільки адреси електронної пошти, що цікавить слідство, окремою задачею є встановлення IP адреси вузла, з якого відправляються електронні листи. Для її вирішення на адресу електронної пошти, що цікавить, надсилається спеціально створений електронний лист, при відкриванні якого, в загальному випадку, встановлюється IP адреса комп'ютеру отримувача.

Спеціальний електронний лист містить приховане посилання на деякий віддалений ресурс, до якого здійснюється автоматичне підключення поштового клієнту при відкритті листа, і відповідно ця

подія фіксується на цьому ресурсі. Створюється або власний віддалений ресурс [3] або використовуються вже готовий сервіс, наприклад ReadNotify (https://readnotify.com/), який пропонує перевірити, чи був прочитаний надісланий електронний лист із встановленням IP-адреси хосту отримувача листа.

Зазначені методи криміналістичного дослідження електронної пошти не є вичерпними і можуть змінюватися з розвитком інформаційних технологій, що у свою чергу потребує безперервного пошуку інструментів і сервісів криміналістичного дослідження електронної пошти.

Список бібліографічних посилань

1. Кіберзлочинність коштує світовій економіці $ 114 млрд на рік // КорреспонденТ: електрон. журн. Дата оновлення: 05.03.2012. URL: http://ua.korrespondent.net/business/web/1326100-kiberzlochinnist-koshtue-svitovij-ekonomici-114-mlrd-na-rik (дата звернення: 07.10.2018).

2. Киберполиция предупреждает о повышении количества киберпреступлений // Телеканал новин «24». Дата оновлення: 14.07.2018. URL: https://24tv.ua/ru/kiberpolicija_preduprezhdaet_o_povyshenii_kolichestva_kiberprestuplenij_n998967 (дата звернення: 09.10.2018).

3. Как узнать айпи адрес чужого компьютера // Компьютерные и интернет технологии... Просто о сложном! URL: http://4aynikam.ru/publ/kak-uznat-aypi-adres-chuzhogo-kompyutera/23-1-0-576 (дата звернення: 10.10.2018).

Одержано 23.10.2018

УДК 343.1+004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7848-6448

ОСОБЛИВОСТІ ОГЛЯДУ ТА ВИЛУЧЕННЯ ДАНИХ З МОБІЛЬНОГО ANDROID ТЕРМІНАЛУ

На сьогодні у рамках розслідувань кримінальних проваджень дуже часто виникає потреба невідкладно, силами оперативних працівників і за дорученням слідчого, здійснювати огляд мобільного терміналу, який було вилучено у підозрюваного на місці вчинення злочину, при обшуку або надано потерпілим. Метою такого огляду є виявлення і фіксація інформації в електронній (цифровій) формі, що містить дані щодо обставин вчинення кримінального правопорушення.

Оскільки оперативні підрозділи Національної поліції мають у своєму розпорядженні невелику кількість коштовних спеціалізованих апаратно-програмних засобів для вилучення даних з мобільних терміналів, наприклад Cellebrite UFED [1], то вочевидь існує необхідність розробки методики вилучення даних із використанням