УДК 343.1+519.7

Вадим Анатолійович КУДІНОВ,
кандидат фізико-математичних наук, доцент,
професор кафедри інформаційних технологій та кібернетичної безпеки
Національної академії внутрішніх справ;
ORCID: https://orcid.org/0000-0002-5299-0590

ОСНОВНІ ПРОГРАМНІ ЗАСОБИ АНАЛІЗУ ВОЛАТИЛЬНИХ ДАНИХ, ЯКІ МОЖНА ВИКОРИСТОВУВАТИ ДЛЯ ОГЛЯДУ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ТА ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ

Національна поліція України має основними завданнями реалізацію державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку [1]. Відповідно до цих завдань, Національна поліція здійснює досудове розслідування кримінальних правопорушень у межах визначеної підслідності тощо [2].

Останніми роками в Україні спостерігається стрімке впровадження майже у всі сфери життєдіяльності суспільства інформаційно-комунікаційних технологій, зокрема, тих, що розширюють можливості реалізації товарів і послуг за допомогою мережі Інтернет. Тому проблема протидії кіберзлочинності та злочинам торгівлі людьми Україну не обходить жодним чином, є вельми актуальною й такою, що вимагає невідкладного вирішення. Враховуючи зазначене органи влади України вживають різноманітні заходи щодо протидії кіберзлочинності та злочинам торгівлі людьми. Так, зокрема, Верховна Рада прийняла Закони України «Про основні засади забезпечення кібербезпеки України» [3] та «Про протидію торгівлі людьми» [4], а Кабінет Міністрів України затвердив План заходів з підтримки розвитку індустрії програмної продукції України на 2018 рік [5], яким передбачено сприяння підвищенню кіберзахисту тощо.

Працівникам органів Національної поліції під час розслідування кіберзлочинів та злочинів, пов'язаних із торгівлею людьми, часто доводиться мати справу із засобами комп'ютерної техніки, які використовуються злочинцями у якості знарядь та засобів вчинення злочинів. При цьому, як зазначено у роботі [6, с. 104], основні інструменти, які можуть знадобитися працівнику Національної поліції для огляду засобів комп'ютерної техніки, є наступними: портативний комп'ютер з автономним джерелом живлення; привод CD-ROM (DVD-ROM); викрутки та інший інструмент; комплекти запасних блоків живлення; диски з операційними системами та іншими програмними

засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду, блокувач жорсткого диску та/або набір дублікаторів, польовий комплект експерта криміналіста тощо. Науковцями та фахівцями-практиками розроблений загальний алгоритм техніки огляду засобів комп'ютерної техніки [6, с. 104], який передбачає на початку своєї реалізації з'ясування питання щодо увімкнення відповідного засобу. Якщо засіб вимкнений, то існує визначений порядок подальшого його огляду. Але якщо засіб працює, то станом на сьогодні в Україні практично не відбувається збирання та документування нестійких волатильних даних (зберігаються в енергозалежних запам'ятовувальних пристроях: оперативній пам'яті, кеші, регістрах), хоча саме волатильні дані часто містять ключі до різних криптоконтейнерів, останні повідомлення у мережі та відкриті документи тощо [6, с. 105]. Це пов'язано, на наш погляд, з відсутністю належної програмно-технічної підготовки з зазначених питань у працівників органів поліції, а також з не визначеністю зі складом та алгоритмом застосування відповідного програмного інструментарію.

Нами проведений аналіз відкритих джерел, відповідно до яких фахівці пропонують такі програмні інструменти Windows для аналізу волатильних даних, які можна використовувати для огляду засобів комп'ютерної техніки, а саме:

PsTools – пакет утиліт, які призначені для більш легкого адміністрування операційних систем Microsoft Windows. Всі утиліти, вбудовані в дистрибутив, не мають графічного інтерфейсу і працюють тільки із командного рядку. Використовувати дані додатки можна для управління локальними, а також віддаленими системами. Пакет установки PsTools містить довідкову службу, в якій представлена повна інформація про використання всіх програм, що входять в дистрибутив.

Dumpit – компактний портативний інструмент, який дозволяє легко зберігати вміст оперативної пам'яті персонального комп'ютера.

FTK – комп'ютерне судово-медичне програмне забезпечення. Сканує жорсткий диск, шукаючи різноманітну інформацію, наприклад, вилучені електронні листи. Включає в себе автономну програму візуалізації диска під назвою FTK Imager. Вона зберігає зображення жорсткого диска в одному файлі або в сегментах, які пізніше можуть бути реконструйовані.

Wireshark – програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний користувацький інтерфейс.

Cygwin – UNIX-подібна середовище та інтерфейс командного рядка для Microsoft Windows. Cygwin забезпечує тісну інтеграцію додатків, даних і ресурсів Windows з додатками, даними і ресурсами UNIX-подібної середовища. З середовища Cygwin можна запускати

звичайні додатки Windows, також можна використовувати інструменти Cygwin з Windows.

Bulk data extractor – комп'ютерний криміналістичний інструмент, який сканує образ диска, файл або каталог файлів та витягує корисну інформацію, не аналізуючи структури файлової системи або файлової системи (виявлення email, IP-адрес, телефонів з файлів). Результати можуть бути легко перевірені, проаналізовані або оброблені автоматичними інструментами. Даний інструмент від інших судово-медичних інструментів своєю швидкістю та ретельністю. Може використовуватися для обробки будь-якого цифрового носія.

Strings – unix-утиліта, що застосовується для пошуку друкованих рядків в бінарних файлах. Вона виводить послідовності друкованих символів, виявлених в заданому файлі. Може використовуватися для візуального аналізу дамп-файлів (core dump) або для відшукання інформації про тип файлу.

MemGator – це інструмент аналізу файлів пам'яті, який автоматизує вилучення даних із файлу пам'яті та складає звіт для дослідника. Об'єднує в програму цілий ряд інструментів.

RegRipper – це криміналістичне програмне забезпечення з відкритим вихідним кодом. Є інструментом вилучення даних реєстру Windows.

Yaru – платформа, незалежна програма для перегляду реєстру Windows.

Registry decoder – це програмний додаток, метою якого є допомогти користувачу проаналізувати, шукати, переглядати та звітувати про вміст вуликів реєстру.

NGrep – це мережевий аналізатор пакетів, є інтерфейс командного рядка. Має можливість шукати регулярний вираз в корисному завантаженні пакета та відображати відповідні пакети на екрані або консолі. Це дозволяє користувачам переглядати весь незашифрований трафік, який проходить через мережу, шляхом встановлення мережевого інтерфейсу в багатонадійний режим.

Event Viewer – це компонент операційної системи Microsoft Windows NT, який дозволяє адміністраторам і користувачам переглядати журнали подій на локальній або віддаленій машині. У Windows Vista корпорація Майкрософт провела реконструкцію системи подій.

PowerForensics – утиліта, що призначена для дослідження жорстких дисків у реальному часі.

Volatility (Volatility Framework) – являє собою набір утиліт для різнобічного аналізу образів фізичної пам'яті. VolUtility – веб-інтерфейс для Volatility framework.

Свій перелік інструментів для збору енергозалежних даних міститься в роботі [6, с. 111].

Висновок. Таким чином, у роботі наведений перелік та призначення основних програмних засобів вільного користування для

аналізу волатильних даних, які можна використовувати для огляду засобів комп'ютерної техніки під час розслідування кіберзлочинів та злочинів торгівлі людьми.

Список бібліографічних посилань

1. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379.

2. Про затвердження Положення про Національну поліцію : постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF (дата звернення: 31.10.2018).

3. Про основні засади забезпечення кібербезпеки : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

4. Про протидію торгівлі людьми : Закон України від 20 вер. 2011 р. № 3739-VI. *Відомості Верховної Ради України*. 2012. № 19-20. Ст. 173.

5. Про затвердження Плану заходів з підтримки розвитку індустрії програмної продукції України на 2018 рік : розпорядження Кабінету Міністрів України від 23 трав. 2018 р. № 344-р. // Кабінет Міністрів України URL: https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-planu-za.

6. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій : навч. курс / [А. Вінаков, В. Гузій, Д. Девіс та ін.]. Київ : Координатор проектів ОБСЄ в Україні, 2017. 148 с.

Одержано 31.10.2018

УДК 004.056.5

Данило Олександрович КУЛІКОВ,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ОЦІНКА БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДОПОМОГОЮ ПЕНТЕСТА

Вступ і постановка проблеми. Процес пентеста включає в себе активний аналіз системи на наявність потенційних вразливостей, які можуть спровокувати некоректну роботу цільової системи, або ж в результаті повну відмову в обслуговуванні.

Важливо виділити мету самого пентеста – це оцінка можливості його здійснення і прогноз економічних трат в результаті успішного здійснення атаки. Результатом є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Тобто, випробування на проникнення є частиною аудиту безпеки.

Слід виділити кілька різних методик випробувань на проникнення. Основними відмінностями є наявність інформації про