Кудінов Вадим Анатолійович, професор кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент

СПЕЦІАЛІЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОВЕДЕННЯ КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ТА ЗБОРУ ЦИФРОВИХ ДОКАЗІВ

Сучасні інформаційні та телекомунікаційні технології, стрімко поширюючись на більшість сфер діяльності людини, змінюють середовище її існування, роблять життя більш комфортним і змістовним. Водночас становлення інформаційного суспільства відбувається не без проблем, найсуттєвішою з яких сьогодні слід вважати кіберзлочинність. Спектр кіберзлочинів різноманітний – від створення комп'ютерних вірусів, вчинення крадіжок, різних видів шахрайства, комп'ютерних підробок до порушення авторських прав та розповсюдження дитячої порнографії. Сьогодні жертвами осіб, які вчиняють злочини у віртуальному просторі, можуть стати не лише окремі люди чи юридичні особи, а й цілі відомства і навіть держави. Зареєстровані випадки так званого кібертероризму, коли комп'ютер використовувався як зброя для блокування важливих систем життєзабезпечення та створення загрози для цілих груп населення. Особливістю таких злочинів є те, що у 90 % випадків злочинці залишаються безкарними. Оскільки жертви або не звертаються в поліцію, або одержують відмову від стражів порядку через небажання чи нездатність надати допомогу.

Для України як однієї з найбільших європейських держав, де у повсякденне життя стрімко входять нові комунікативні технології, зокрема ті, що розширюють можливості реалізації товарів і послуг за допомогою мережі Інтернет, проблема кіберзлочинності не обходить жодним чином. Таким чином, для України проблема поширення кіберзлочинності сьогодні є вельми актуальною й такою, що вимагає невідкладного вирішення. Кіберзлочинність, без перебільшення, стала одним з основних викликів, що постають перед сучасним суспільством.

Враховуючи зазначене органи влади України вживають різноманітні заходи щодо протидії кіберзлочинності. Так, зокрема, Верховна Рада України 05 жовтня 2017 року підтримала законопроект «Про основні засади забезпечення кібербезпеки України» (№ 2126 а) – у другому читанні та в цілому, а Кабінет Міністрів України 31 травня 2017 року затвердив План заходів з підтримки розвитку індустрії програмної продукції України на 2017 рік [1]. Відповідно до п.п. 1 п. 1 цього Плану сьогодні розроблений проект Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо використання інформації в електронній (цифровій) формі як доказу під час здійснення кримінального провадження», яким передбачено оптимізацію процесу збору інформації в електронній (цифровій) формі та надання їй належної правової оцінки як джерелу доказів у кримінальному провадженні. Відповідно до п.п. 2 п. 1 цього Плану Центральні органи виконавчої влади до 01 листопада поточного року повинні були визначити порядок сертифікації програмно-апаратних засобів, що використовуються для виявлення, фіксації, вилучення та дослідження доказів під час здійснення кримінального провадження у справах щодо злочинів, вчинених із застосуванням інформаційно-комунікаційних технологій.

Ураховуючи зазначене, виникає актуальне питання щодо вибору спеціалізованого програмного забезпечення для проведення криміналістичного аналізу та збору цифрових доказів.

Нами проведений аналіз відкритих джерел, відповідно до яких фахівці пропонують такий програмний інструментарій для використання [2; 3]:

*Фреймворки**:***

– dff (Digital Forensics Framework) – платформа з відкритим вихідним кодом для проведення робіт по вилученню і дослідженню даних, можна використовувати для дослідження жорстких дисків і енергозалежної пам'яті, створення звітів про користувача і системні дії;

– PowerForensics – утиліта, що призначена для дослідження жорстких дисків у треальному часі;

– The Sleuth Kit (TSK) – це бібліотека на мові С і набір інструментів командного рядка, які дозволяють досліджувати образи дисків;

Реал-тайм утиліти:

– grr (GRR Rapid Response) – інструмент для розслідування і аналізу інцидентів;

– mig (Mozilla InvestiGator) – це платформа для проведення оперативних досліджень на віддалених кінцевих точках, дозволяє дослідникам паралельно отримувати інформацію з великої кількості джерел, прискорюючи тим самим розслідування інцидентів та забезпечення безпеки повсякденних операцій.

Робота з образами (створення, клонування):

– dc3dd – поліпшена версія консольної утиліти dd;

– adulau / dcfldd – ще одна поліпшена версія dd;

– FTK Imager – перегляд і клонування носіїв даних в середовищі Windows;

– Guymager – перегляд і клонування носіїв даних в середовищі Linux.

Вилучення даних:

– bstrings – п оліпшена версія популярної утиліти strings;

– bulk_extractor – виявлення email, IP-адрес, телефонів з файлів;

– floss – ця утиліта використовує розширені методи статичного аналізу для автоматичної деобфускації даних з довічних файлів шкідливих програм;

– photorec – мультисистемна платформа для пошуку і вилучення файлів з образів операційних систем, компакт-дисків, карт пам’яті, цифрових фотокамер і т.ін. Основне призначення – вилучення знищених (або втрачених) файлів.

Робота з RAM:

– inVtero.net – фреймворк, що відрізняється високою швидкістю роботи;

– KeeFarce – витяг паролів KeePass з пам’яті;

– Rekall – аналіз дампов RAM, написаний на python;

– volatility (Volatility Framework) – являє собою набір утиліт для різнобічного аналізу образів фізичної пам’яті;

– VolUtility – веб-інтерфейс для Volatility framework.

Мережевий аналіз:

– SiLK Tools – інструменти для аналізу трафіку для полегшення аналізу безпеки великих мереж, ідеально підходить для аналізу трафіку на магістралі або кордоні великого, розподіленого підприємства або провайдера середнього розміру;

– Wireshark – один з найпопулярніших аналізаторів пакетів, може бути ефективно використаний для аналізу трафіку (в тому числі і шкідливого), функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, однак Wireshark має графічний інтерфейс користувача і набагато більше можливостей із сортування та фільтрації інформації, дозволяє користувачеві переглядати весь мережевий трафік в режимі реального часу.

Артефакти Windows:

– FastIR Collector – великий збирач інформації про систему Windows (реєстр, файлова система, сервіси, автозавантаження і т.ін.);

– FRED – кросплатформений аналізатор реєстру Windows.

Hex редактори:

– 0xED – HEX редактор OS X;

– Hexinator – Windows версія Synalyze It;

– HxD – маленький і швидкий HEX редактор.

Конвертори:

– CyberChef – мультіінструмент для кодування, декодування, стиснення і аналізу даних;

– DateDecode – конвертація бінарних даних.

Фахівці радять під час проведення робіт з дослідження і збору цифрових доказів дотримуватися принципів незмінності, цілісності, повноти інформації та її надійності. Для цього необхідно дотримуватись рекомендацій до використання програмного забезпечення і методів проведення розслідувань.

Список використаних джерел

1. Про затвердження Плану заходів з підтримки розвитку індустрії програмної продукції України на 2017 рік [Електронний ресурс] : розпорядження Кабінету Міністрів України від 31 трав. 2017 р. № 367-р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/367-2017-%D1%80. – Назва з екрана.

2. Компьютерная криминалистика (форензика): подборка полезных ссылок [Электронный ресурс]. – Режим доступа: https://m.habrahabr.ru/company/pentestit/blog/338378/.com/. – Загл. с экрана.

3. Компьютерная криминалистика (форензика) – обзор инструментария и тренировочных площадок [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/pentestit/blog/327740/. – Загл. с экрана.