УДК 004.62

Сергій Олександрович Бичков,
заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Штатні засоби криптографічного захисту інформації користувача в операційних системах Microsoft Windows та MAC OS

На сьогодні найбільш поширені операційні системи, які обирають користувачі для своїх персональних комп'ютерів це Windows 10 та операційна система Mac OS для комп'ютерів компанії Apple. З приводу захисту особистих даних користувачів операційних систем розробники вбудували в них програмне забезпечення, що дозволяє застосувати алгоритми криптографічного захисту. Для операційних систем Windows 10 це BitLocker, для операційних систем Mac OS – це FileVault 2. Підхід який пропонується для подолання встановленого криптографічного захисту в цих зазначених операційних системах у більшому схожий але має деякі особливості з використанням стороннього програмного забезпечення та послідовністю дій на активній операційній системі, які необхідно буде виконати особі, що проводить вилучення комп'ютерної техніки.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Windows 10.

Розробники операційних систем сімейства Windows, починаючи з версії Microsoft Windows Vista Максимальна\Корпоративна додали у функціонал своїх продуктів можливість шифрування логічних розділів диску (томів) за допомогою вбудованого в операційну систему програмного забезпечення BitLocker, який підтримує наступні алгоритми шифрування:

- AES 128,
- AES 128 с Elephant diffuser (використовується за замовченням),
- AES 256,
- AES 256 с Elephant diffuser,

- XTS-AES (починаючи з Windows 10 версії 1511).

Для того щоб зрозуміти ввімкнено шифрування чи ні, на активній системі персонального комп'ютера чи ноутбука, що буде вилучатися для направлення на комп'ютерно-технічну експертизу, самий простий спосіб це увійти в меню провідник або увійти в «Цей комп'ютер» (російською «Этот компьютер»), на панелі де відображається список логічних дисків можна побачити іконки логічних дисків. Логічні диски до яких застосовано шифрування за допомогою BitLocker мають іконку у вигляді зображення диску та замку біля нього. Якщо замок відчинений це означає що диск замонтовано до системи, якщо зачинений – диск не замонтовано, та для того щоб отримати доступ до даних що на ньому зберігаються необхідно ввести пароль або використати апаратний ключ.

У разі, якщо застосовано шифрування функцією BitLocker, подальшим кроком, який є дуже важливим для успішного проведення дослідження у майбутньому є зняття дампу (копії) ОЗУ.

Дамп ОЗУ на комп'ютерах з операційною системою Windows можливо виготовити за допомогою спеціального програмного забезпечення, наприклад, «AccessData FTK Imager Lite Version», «Belkasoft Live RAM Capturer», «Magnet RAM Capture» та іншого. Наведене програмне забезпечення є безкоштовним та легким в користуванні.

Дуже важливо зробити дамп ОЗУ не даючи змоги власнику персонального комп'ютера його вимкнути, оскільки ОЗУ це енергозалежна пам'ять, та після вимикання комп'ютера більшість важливих даних, які містилися в неї, будуть очищені.

Таким чином, алгоритм дій має наступні ключові кроки:

1. Пересвідчитися чи застосовано до носіїв інформації комп'ютерної техніки функція шифрування даних BitLocker,

2. У разі якщо застосовано, виготовити дамп (копію) ОЗУ цього комп'ютера,

3. Надати судовому експерту для дослідження вилучену комп'ютерну техніку та виготовлений з неї дамп ОЗУ.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Mac OS

На відміну від попередньої версії функції FileVault, яка могла захистити шифруванням лише розділ користувача, FileVault 2 здатна шифрувати як розділ диску, так і весь диск.

На стадії вилучення комп'ютерної техніки Apple, якщо вона знаходиться в активному стані (операційна система запущена, здійснений вхід до облікового запису користувача) необхідно виготовити дамп ОЗУ та надати його для подальшого дослідження експерту разом із комп'ютерною технікою, що вилучається.

Існує декілька сторонніх засобів для виготовлення дампів ОЗУ з комп'ютерів під керуванням операційною системою Mac OS, це:

1. Goldfish,

2. Mac Memory Reader,

3. OSXPMem,

які зможуть стати в нагоді при виготовленні дампів ОЗУ на версіях Mac OS до Mac OS X El Capitan 10.11.

Таким чином, у разі якщо виготовлення дампу ОЗУ з активної системи комп'ютера під керуванням операційної системи Mac OS завершилось успіхом, як і у випадку з операційними системами Windows, виготовлена копія пам'яті надається разом із технікою що вилучається на комп'ютерно-технічну експертизу для подальшого дешифрування та дослідження інформації судовими експертами.

Одержано 21.10.2019