All software of expert forensic activity is proposed to be classified in the following way: programs for automating the search for criminalistic information; software products that automate the process for detecting and researching the features of objects; special programs for evaluating the distinguished features of various research objects; programs that allow to automate the process of drawing up an expert opinion. At the same time, such a classification does not pretend to be completely unconditional and full; in the future it can be supplemented and improved.

The next processes are highlighted: the formation and development of foreign and domestic software products, automated workplaces, software and hardware complexes, opportunities, disadvantages and prospects of their use in conducting separate types of forensic examinations: from handwriting, fingerprinting to explosive engineering.

УДК 343.98

Г. В. Куцо
старший науковий співробітник

Одеський науково-дослідний інститут судових експертиз
Міністерства юстиції України

С. О. Юлов
завідувач відділу

Одеський науково-дослідний інститут судових експертиз
Міністерства юстиції України

ДОСЛІДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ТЕРМІНАЦІЇ VoIP ТРАФІКУ (РЕФАЙЛІНГУ), ПОБУДОВАНОГО НА БАЗІ МОДЕМІВ HUAWEI

В цій статті містяться базові відомості щодо організації системи рефайлінгу (термінації VoIP трафіку), розглянуто необхідне для цього апаратне та програмне забезпечення. Стисло розглянуто загальновживане програмне забезпечення, яке використовується для організації рефайлінгу. Вказане програмне забезпечення та наведена інструкція до його використання для уникнення блокування обладнання з боку операторів стільникового зв'язку.

Під «рефайлінгом» розуміють підміну міжнародного трафіку на локальний, шляхом перенаправлення VoIP[15] дзвінка з-за кордону в місцеву

[15] IP-телефонія, (вимовляється «айпі-телефонія») — телефонний зв'язок по протоколу IP. Під IP телефонією розуміється набір комунікаційних протоколів, технологій та методів, що забезпечують традиційні для телефонії набір номера, дозвон і двостороннє голосове спілкування, а також відео-спілкування по мережі інтернет або будь-яким іншим USB-хаби IP-мережами. Сигнал по каналу зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискається) для того, щоб видалити надлишок інформації та знизити навантаження на мережу передачі даних.

GSM мережу, що правоохоронними органами трактується як порушення встановленого порядку маршрутизації (ст. 361 КК України). Виклик тарифікується як місцевий, а різниця у вартості становить заробіток організаторів.

Термін «рефайл» частіше використовується з негативним забарвленням. GSM оператори щорічно зазнають великих збитків внаслідок термінації[16], які обчислюються в мільйонах доларів. Тому вони готові вкладати великі суми грошей в розробку спеціальних програмних рішень, які відстежують рефайлінг. AntiFraud системи можуть бути аналітичними та на дозвон. Перші аналізують активність абонента в мережі, другі здійснюють дзвінки на номера, по відношенню до яких є підозри у термінації трафіку. При виявленні рефайлінга системи блокують абонентські номери.

Бізнес в сфері термінації трафіку — надприбутковий, в місяць він може приносити прибуток близько $ 2000, при наявності мінімального комплекту обладнання — кількох VoIP шлюзів. Для старту потрібні мінімальні інвестиції, при цьому вкладені гроші швидко окупаються. В середньому знадобиться на це 2–6 місяців.

Актуальність цієї статті пов'язана з тим, що відсутня методика проведення експертиз та досліджень телекомунікаційного обладнання термінації з застосуванням модемів марки Huawei при здійснені правопорушень пов'язаних з підміною міжнародного трафіку на локальний, шляхом перенаправлення VoIP дзвінка з-за кордону в місцеву GSM мережу.

1. Апаратні засоби побудови телекомунікаційного вузлу термінації міжнародних дзвінків з застосуванням модемів марки Huawei.

Для побудови телекомунікаційного вузлу термінації зазвичай використовують модеми «Huawei» (див. рис. 1), SIM-картки операторів зв'язку, GSM-шлюзи (див. рис. 2), USB-концентратори, персональні комп'ютери, ноутбуки, нетбуки.

Рис. 1

[16] Під термінацією розуміється перенаправлення телефонного виклику з мережі VoIP у локальну або стільникову мережу телефонного зв'язку.

Рис. 2

2. Програмні засоби побудови телекомунікаційного вузлу термінації міжнародних дзвінків з застосуванням модемів марки Huawei.

Телекомунікаційний вузол термінації будують за схемами, показаними на рис. 3 та 4.

Рис. 3

Рис. 4

Зазвичай, для організації телекомунікаційного вузлу термінації використовують програмне забезпечення:

- «**Oktell SipGsmGateway**», який при встановленні в середовищі операційних систем Microsoft Windows розташовується в теці «/Program Files (x86)/SipGsmGateway». Це ПЗ є програмним шлюзом[17] для зв'язку між мобільними GSM[18] — мережами та корпоративною АТС[19], використовується для організації голосового з'єднання між мережами GSM и VoIP (протокол SIP). Шлюз встановлюється на комп'ютер з Windows. Для підключення до мережі GSM потрібні USB-модеми.

Використання програмного забезпечення «Oktell SIP-GSM» надає можливість «перебуваючи за межами офісу, телефонувати в будь-яку точку світу з мобільного телефону за тарифами встановленими провайдером та оператором (або операторами) стільникового зв'язку». «Oktell SIP — GSM» шлюз — з використанням до 10 каналів зв'язку розповсюджується безкоштовно.

Це програмне забезпечення («Oktell SIP– GSM») може використовувати наступні моделі модемів: Huawei E1550, Huawei E160g, Huawei E173, ZTE MF180, Huawei E1752C. Не виключається робота і з іншими моделями виробника Huawei.

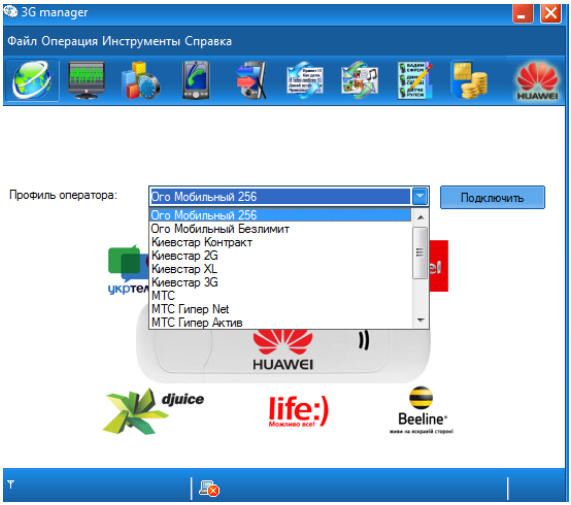

Рис. 5

---

[17] Програмне забезпечення, покликане організувати передачу трафіку між різними мережами. Програма є робочим інструментом системного адміністратора, дозволяючи йому контролювати трафік і дії співробітників.

[18] GSM (от названия группы Groupe Spécial Mobile, позже переименован в Global System for Mobile Communications) (русск. СПС 900) — глобальный стандарт цифровой мобильной сотовой связи, с разделением каналов по времени (TDMA) и частоте (FDMA).

[19] Автоматична телефонна станція.

- «**3G manager**» 3G Modem Manager (див. рис. 5) — програма для роботи з 3G модемами HUAWEI і деякими моделями модемів 3G від австралійського виробника ZTE. За допомогою цієї утиліти можна налаштувати 3G модем на роботу з сім-картами інших операторів стільникового зв'язку, якщо модем не заблокований (залочений) на апаратному рівні. Крім цього можливо завжди бачити рівень сигналу мережі, враховувати витрати інтернет трафіку, дізнатися реальну швидкість інтернет 3G модема, включати і вимикати інтернет на 3g модемі за розкладом за допомогою зручного планувальника. У програмі вже забиті точки доступу (APN) операторів стільникового зв'язку Росії і України (beeline, mts, tele2, nts, kyivstar та ін.). Можливо в будь-який момент дізнатися баланс на сім-карті, послати USSD-запит на підключенні будь-якої послуги, включити і вимкнути PIN код на SIM-картці 3G модема, переглядати отримані SMS.

- «**SipAssistent**» (див. рис. 6) — подібна за функціональними здібностями до 3G Modem Manager, однак одночасне виконання цього програмного забезпечення не рекомендовано.

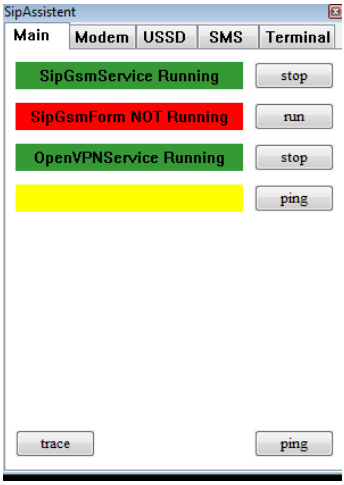

Рис. 6

2. Особливості використання програмного забезпечення «Oktell SIP-GSM».

Виробником передбачено, що крім режиму модему з використанням офіційного програмного забезпечення цей пристрій дозволяє здійснювати телефонні виклики як при використанні звичайного стільникового терміналу (для цього користувачу необхідна гарнітура). У разі використання у якості SIP GSM шлюзу програмне забезпечення SIP сервера SipAssistent або/та 3G Modem Manager здійснює виклик та перенаправляє голосові данні між VoIP та GSM-мережею.

Програма, що реалізує зазначений функціонал називається Oktell SIP GSM Gateway. Програмний шлюз працює як сервіс ОС Windows, використовує можливості драйверу модему (подає АТА команди) та виступає стандартним SIP шлюзом. SipAssistent або/та 3G Modem Manager взаємодіє з ним як зі стандартним SIP шлюзом (Generic SIP Gateway), приймаючи і передаючи голосові виклики в GSM мережу і назад.

Huawei модеми офіційно поставляються в Україну, і, отже, знаходяться в «білому» списку Укрчастотнагляді, на відміну від багатьох інших аналогічних пристроїв. Можливо нарощувати або розподіляти кількість GSM каналів простим додаванням нових модемів Huawei. «Апаратні» шлюзи завжди йдуть з фіксованим числом портів, крім того, ці порти не можна «рознести» в різні місця, якщо того вимагає топологія мережі.

3. Зміна IMEI номерів модемів Huawei.

При виявлені свічень рефайлу, оператори мобільного зв'язку вносять до сірого списку IMEI номери, або блокують ці IMEI. В результаті модем телекомунікаційної системи рефайлу не працює. Зазвичай, якщо не змінювати IMEI модему, блокування роботи операторами мобільного зв'язку складає від трьох діб до місяця. З метою недопущення блокування роботи модемів, зловмисниками, здійснюється періодична процедура зміни IMEI.

Для зміни IMEI в модемах Huawei, зазвичай, використовується програмне забезпечення «imei-recovery-template-huawei-e173.exe», або «imei-recovery-template-huawei-e1550.exe».

Процес зміни IMEI не складний і не вибагливий. При запуску програмного забезпечення зміни IMEI користувачу необхідно погодитись з ліцензійними угодами (див. рис. 7) після чого розпочнеться процес зміни (перепрошиви), який завершується повідомленням про успішне виконання (див. Рис.8 та 9).

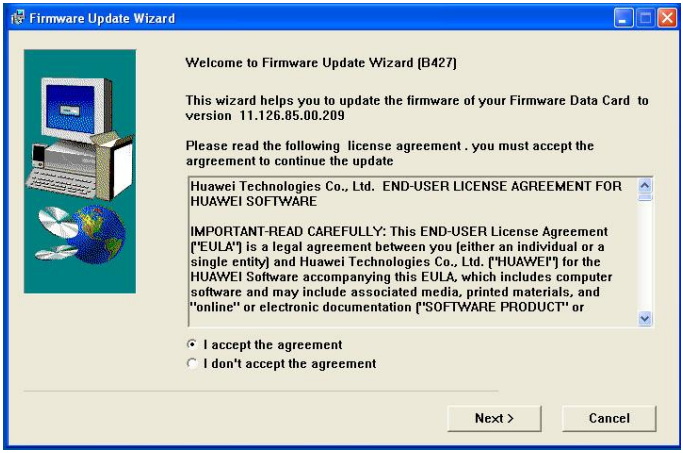

Рис. 7

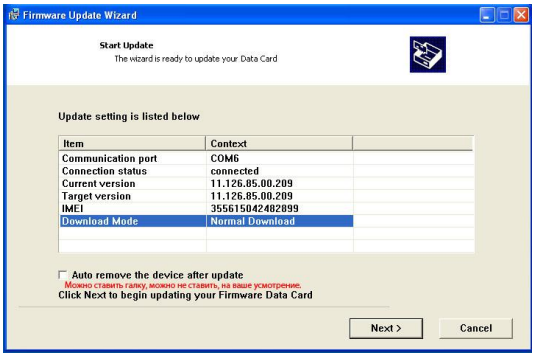

Рис. 8

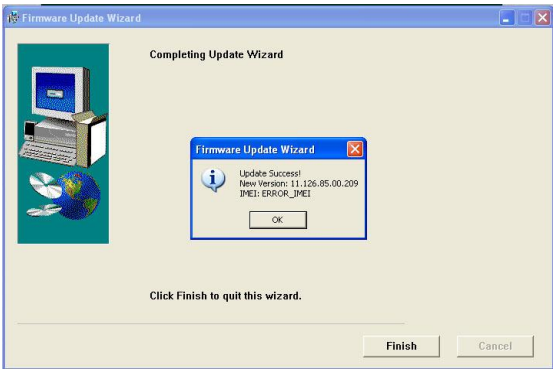

Рис. 9

В разі активності роботи програмного забезпечення «3G manager» або «Oktell SIP-GSM» виникає повідомлення про помилку (див. рис. 10).

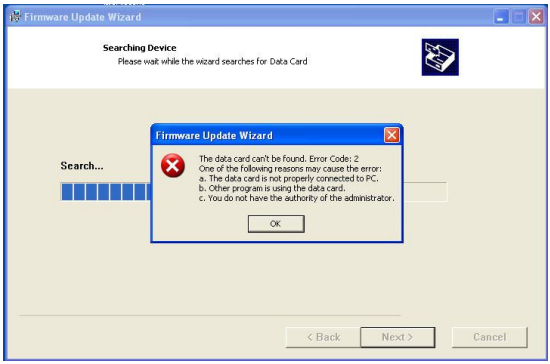

Рис. № 10

Після закриття «3G manager» або «Oktell SIP-GSM» слід запустити процес зміни IMEI повторно.

Перелік посилань

1. *Нелегальная* телефонная сеть [Електронний ресурс]. Режим доступу: https://www.kramatorsk.info/talk/index.php?topic=4288.0.
2. *С рефайлом борются* всем миром [Електронний ресурс]. Режим доступу: http://www.dsnews.ua/politics/art1819.
3. *Что такое рефайлинг* голосового трафика? [Електронний ресурс]. Режим доступу: https://goantifraud.com/ru/blog/529-chto-takoe-refayling-golosovogo-trafika.html.
4. *Перевірка коду* IMEI [Електронний ресурс]. Режим доступу: Інтернет-ресурс http://www.ucrf.gov.ua/perevirka-imei-2/.
5. *Обсуждение* Huawei E3531 (МТС 423S, Мегафон M21-4) [Електронний ресурс]. Режим доступу: http://4pda.ru/forum/lofiversion/index.php?t553049-180.html.
6. *Oktell* SIP-GSM Gateway и Asterisk [Електронний ресурс]. Режим доступу: https://kovalyshyn.pp.ua/439.html.
7. *Универсальная* программа для 3g модема [Електронний ресурс]. Режим доступу: http://compprogramm.ru/stati/universalnaya-programma-dlya-3g-modema/
8. *GSM-шлюз* [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/GSM-шлюз.

ИССЛЕДОВАНИЕ ТЕЛЕКОМУНИКАЦИОННОГО ОБОРУДОВАНИЯ ТЕРМИНАЦИИ VoIP ТРАФИКА (РЕФАЙЛИНГА), ПОСТРОЕННОГО НА БАЗЕ МОДЕМОВ HUAWEI

Г. В. Куцо
С. О. Юлов

В представленной статье рассмотрена актуальная проблема экспертного исследования системы рефайлинга (терминации VoIP трафика), принципы построения и наиболее часто используемое для таких систем оборудование. С законодательной точки зрения организация рефайлинга является нарушением установленного порядка маршрутизации междугородних и международных телефонных соединений, что приводит к существенному ущербу для операторов связи и, в конечном итоге, к ущербу государства в виде недополученных налоговых отчислений. Суммарный ущерб от использования таких систем может оцениваться в миллионы долларов ежегодно.

На сегодняшний день в экспертной практике Украины отсутствуют методики для исследования данного вида систем. В том числе нет даже систематизированных методических подходов к их исследованию, что обусловливает актуальность статьи и её пользу в экспертной практике и как уже готовую к применению инструкцию по исследованию, и как базу для дальнейшего развития методических подходов в отношении данного вида объектов исследований.

Статья затрагивает наиболее употребительное оборудование для рефайлинга и не является подробной и детализированной инструкцией. Но, в то же время, изложенные в статье принципы позволяют эксперту с лёгкостью определиться с направлением исследования в случае, когда на исследование поступает оборудование отличное от описанного в данной статье. Не смотря на то, что операторы связи, со своей стороны, пытаются противодействовать работе систем рефайлинга с целью блокирования их работы — злоумышленники, со своей стороны, используют методы обхода противодействия операто-

ров. В данной статье рассмотрены частоупотребимые методы обхода и описано используемое для этого программное обеспечение и подходы работы системы рефайлинга.

Ядром системы рефайлинга является персональный компьютер, в памяти которого остаются определённые следы как вызванные работой самой системы, так и оставляемые злоумышленником, который её обслуживал. В статье изложены подходы к поиску и выявлению данных следов.

RESEARCH OF TELECOMMUNICATION EQUIPMENT VoIP TERMINATION OF A TRAFFIC (REFILING) CONSTRUCTED ON THE HUAWEI MODEM BASIS

H. Kutso
S. Yulov

The article deals with the actual problem of expert research of the system of refilling (termination of VoIP traffic), principles of construction and the equipment most often used for such systems. From the legislative point of view, the organization of refiling is a violation of the established procedure for routing long-distance and international telephone connections, which leads to significant damage for telecom operators and, ultimately, to a state's damage in the form of lost tax deductions. The total damage from the use of such systems can be estimated in millions of dollars annually.

Currently, in the expert practice of Ukraine there are no methods for studying this type of systems. In particular, there are not even systematized methodological approaches to their research, which makes the article relevant and useful in expert practice and as a ready-to-use research manual and as a basis for further development of methodological approaches to this type of research objects.

The article covers the most common refiling equipment and it is not a detailed instruction. But, at the same time, the principles stated in the article allow the expert to easily determine the direction of the research in the case when experts receive for the research the equipment different from that described in this article. In spite of the fact that communication operators, for their part, are trying to counteract the work of the refiling systems in order to block their work — the attackers, for their part, use methods to bypass the operators' counteraction. This article discusses commonly used methods of circumvention and describes the software used and the approaches of the refiling system for this purpose.

The core of the refiling system is a personal computer, in memory of which there are certain tracks as caused by the operation of the system itself, and left by the attacker who served it. The article describes the approaches to the search and identification of these tracks.