Mobile Forensics Day 2020
Сентябрь 2020, Москва

ELCOMSOFT

Современные методы извлечения данных из Apple iPhone

Извлечение данных из iPhone

Содержание

Способы извлечения данных

- Расширенное логическое извлечение
- Извлечение посредством джейлбрейка
- Использование уязвимости в загрузчике
- Извлечение без джейлбрейка

Извлечение данных из iPhone

Проблемы и задачи

- Пасскод неизвестен
- Устройство заблокировано после 10 неверных попыток
- Устройство сброшено до заводских настроек
- Пасскод не установлен или известен, необходимо максимально полное извлечение данных
- Устройство повреждено и не полностью работоспособно
- Программный сбой (например, после неудачного обновления), устройство не загружается
- Доступа к облачным данным нет, либо они отсутствуют или недостаточны
- Возможно, устройство в режиме пропажи или послана команда на удаление данных
- Некоторые данные на устройстве зашифрованы (например, переписка Signal)
- Некоторые данные удалены с устройства
- Необходим полноценный анализ

Извлечение данных из iPhone

Эти методы не работают

- JTAG: отладочный порт доступен только на инженерных образцах
- Извлечение микросхемы памяти: шифрование делает этот метод бесполезным (на моделях с Secure Enclave)

Извлечение данных из iPhone

Методы извлечения данных

- **Расширенное логическое извлечение**
  - Резервные копии (с паролем или без); в резервных копиях с паролем – часть содержимого связки ключей
  - Медиа-файлы (включая метаданные) и открытые данные приложений
  - Журналы crash & diagnostic logs
- **«Физическое» извлечение**
  - Полный образ файловой системы
  - Полное содержимое связки ключей (пароли, токены и ключи шифрования)

Извлечение данных из iPhone

Расширенное логическое извлечение

- Резервная копия может быть зашифрована паролем
  - iOS 11/12/13 позволяет сбросить пароль (необходим пасскод)
    - не всегда; может помешать пароль Restrictions/ScreenTime
    - часть данных теряется из-за сброса пасскода
  - Медленный перебор (~100 п/с на GPU); результат не гарантирован
- Для связи с устройством можно использовать lockdown-записи
  - Режим ограничений USB делает логическое извлечение невозможным
- Медиа-файлы (включая метаданные) и журналы диагностики доступны даже при установленном пароле на резервную копию
- Рекомендуется установить диагностические профили:
  - https://developer.apple.com/bug-reporting/profiles-and-logs/
- Часть функционала доступна также для Apple TV и Apple Watch
- Могут быть проблемы с managed-устройствами (MDM)

Физическое извлечение данных

Чего нет в резервных копиях

- Данные приложений, для которых запрещено резервное копирование
- Все записи связки ключей, включая защищённые
- Статистика загрузки CPU
- Статистика использования аккумулятора
- Использование данных и сетевых ресурсов
- Многочисленные журналы и логи активности системных компонентов и пользовательских приложений
- WAL-файлы для всех баз данных SQLite (возможен доступ к некоторым удалённым записям)

Физическое извлечение данных

Достоинства метода

- Максимально полный доступ к данным
- Почта, переписка во всех программах мгновенного обмена сообщениями (возможно дополнительное шифрование)
- Доступ к данным всех приложений (возможно дополнительное шифрование)
- Расширенная история местоположения
- Детальная история использования телефона
- **Можно полностью расшифровать Связку ключей (keychain)**

Извлечение данных из iPhone

Особенности физического извлечения данных

- **Требуется низкоуровневый доступ к файловой системе**
  - Способ 1: установка джейлбрейка
  - Способ 2: использование аппаратной уязвимости в bootrom
  - Способ 3: использование программы-агента

Извлечение данных из iPhone

Особенности физического извлечения данных

- **Способ 1: установка джейлбрейка**
  - Есть риски (нежелательная модификация системного раздела, установка на устройство нежелательного ПО и т.п.)
  - После удаления остаются следы, а нормальная работа устройства может быть нарушена
  - Может потребоваться учётная запись разработчика
  - Возможна установка с enterprise-сертификатом или через AltStore
  - Может понадобиться установка ssh-клиента
  - **Административный запрет в ряде организаций**

Извлечение данных из iPhone

Особенности физического извлечения данных

- **Способ 2: использование аппаратной уязвимости в bootrom**
  - Аппаратная уязвимость существует в устройствах поколений A4-A11 (iPhone 4…iPhone X, соответствующие модели iPad, Apple TV)
  - Не зависит от версий iOS, не может быть исправлена
  - iPhone 5s и старше: эксплойт checkm8, джейлбрейк checkra1n
  - **Вариант 1**: эксплуатация checkm8 для доступа к файловой системе и связке ключей
  - **Вариант 2**: работа через джейлбрейк checkra1n
  - Частичная поддержка устройств с неизвестным паролем
- Минимальная версия iOS: 12.3
- Максимальная версия iOS: 13.7 (поддержка iOS 14 под вопросом; BFU-извлечение из устройств с неизвестным пасскодом скорее всего будет невозможно)

Извлечение данных из iPhone

Особенности физического извлечения данных

- **Способ 3: использование программы-агента**
  - Не требует установки джейлбрейка
  - Максимальная безопасность, работоспособность устройства не может быть нарушена
  - Высокая скорость работы (~2 GB/min)
  - После удаления не оставляет явных следов
  - Возможно использование обычной учётной записи Apple ID, регистрация в программе Apple для разработчиков не обязательна (*только на macOS*)
  - Совместимость с iOS от 9.0 до 13.5
  - Поддержка A12/A13 (iPhone Xr, iPhone Xs, iPhone 11, iPhone SE 2020)

Физическое извлечение данных

Способ 1: инструменты

- Файл с jailbreak для версии устройства и iOS
- Cydia Impactor для установки jailbreak
- Учётная запись разработчика Apple
- *(Альтернатива)* https://ignition.fun
- *(Альтернатива) AltStore*

Недостатки:

- Низкая надёжность
- Остаются следы использования
- Необходимость установки ssh-клиента (для некоторых джейлбрейков)

Физическое извлечение данных

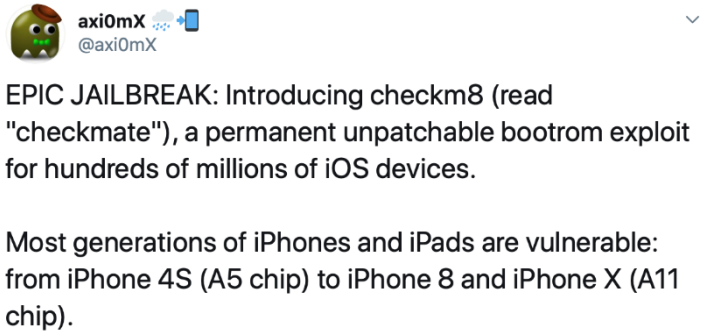
Способ 2: с использованием аппаратной уязвимости

- Использует аппаратную уязвимость в Bootrom (limera1n / checkm8)
- Совместим с большинством версий iOS
- Извлечение с использованием джейлбрейка или без него
- Установка через режим DFU
- В отличие от классических типов джейлбрейков, обходит режим ограничений USB
- Возможно частичное извлечение файловой системы и связки ключей из iPhone с неизвестным паролем
- Частичное извлечение даёт доступ к сильно ограниченному набору данных

Использование джейлбрейк

Эксплойт Checkm8

- Опубликован в сентябре 2019
- Использует аппаратную уязвимость в Bootrom
- **Apple не сможет его исправить (but…)**
- Поддерживает процессоры A5 - A11
- iPhone 5S до iPhone X включительно
- (теоретически) поддержка всех iOS



Использование джейлбрейк

Джейлбрейк Checkra1n

- Джейлбрейк основан на эксплойте checkm8
- Устанавливается в режиме DFU
- Не требует Cydia Impactor
- *Порт USB в режиме DFU всегда доступен независимо от активации режима ограничений USB*
- Позволяет извлекать многие файлы и базы данных в режиме «холодной» загрузки (до первой разблокировки)
- *НЕ МОЖЕТ использоваться для взлома кода блокировки*
- Если код блокировки известен, позволяет извлечь образ файловой системы и расшифровать связку ключей

Проблемы

- Как и классические утилиты джейлбрейк, модифицирует системный раздел
- Не работает с iOS ниже 12.3
- **Могут быть проблемы с iOS 14**

Физическое извлечение данных

Способ 3: с использованием программы-агента

- Использование агента собственной разработки позволяет избежать всех проблем, связанных с установкой джейлбрейка
- Максимальная надёжность работы, отсутствие рисков
- Минимальные следы использования (только записи в системных журналах)
- Работоспособность устройства не нарушается, обновления OTA устанавливаются в штатном режиме
- Для работы требуется код блокировки устройства
- Для установки требуется учётная запись Apple ID, зарегистрированная в программе Apple для разработчиков

Физическое извлечение данных

Ограничения метода (агент)

- Требуется прямой доступ к файловой системе, а следовательно – эскалация привилегий
- Требуется пароль блокировки (пасскод)
- **Эскалация привилегий доступна далеко не для всех платформ и версий iOS (на данный момент до 13.5)**
- *Желательно* использование учётной записи разработчика Apple

Использование программы-агента

Извлечение данных без джейлбрейка

- Программа-агент собственной разработки Элкомсофт
- Агент (файл IPA) подписывается сертификатом разработчика и устанавливается на устройство
- Агент запускается на устройстве
- Агент использует известные уязвимости для эскалации привилегий
- С компьютера эксперта подаётся команда извлечения данных
- Не используется ssh (выше скорость и надёжность)
- Файловая система упаковывается в архив TAR
- Извлекается и расшифровывается Связка ключей
- Агент удаляется с устройства
- Устройство функционирует в штатном режиме
- Единственный след от использования агента – записи в системных журналах

Совместимость

	iPhone	iPad				BFU	Unlock	FFS+keychain	
			Mini	*Air*	*Pro*			*limera1n/checkm8*	*agent*
A4	iPhone 4	1				+	+	+	-
A5/A5X	iPhone 4s	2, 3	1			*	*	*	-
A6/A6X	iPhone 5, iPhone 5c	4				+	+	*	-
A7	iPhone 5s		2, 3	1		+	-	iOS 12.3 - 12.4.8	iOS 9.0 - 12.4.8
A8/A8X	iPhone 6		4	2		+	-	iOS 12.3 - 12.4.8	iOS 9.0 - 12.4.8
A9/A9X	iPhone 6s, iPhone SE	5			1	+	-	iOS 12.3 - 13.7	iOS 9.0 - 13.5
A10/A10X	iPhone 7	6, 7			2	+	-	iOS 12.3 - 13.7	iOS 10.0 - 13.5
A11	iPhone 8, iPhone X					+	-	iOS 12.3 - 13.7	iOS 11.0 - 13.5
A12/A12X/A12Z	iPhone Xr, iPhone Xs		5	3	3, 4	-	-	-	iOS 12.0 - 13.5
A13	iPhone 11, iPhone SE2					-	-	-	iOS 13.0 - 13.5

- Green: 32-битные модели, практически неограниченные возможности
- Blue: применим эксплойт checkm8, возможно BFU-извлечение
- Red: возможна работа только с разблокированными устройствами

- BFU: Before First Unlock, [частичное] извлечение при неизвестном пасскоде
- Unlock: Взлом пасскода (4 или 6 цифр – гарантированно) и снятие блокировки после 10 неверных попыток
- FFS: Full File System, полный образ файловой системы (плюс связка ключей)

Ресурсы для экспертов

Скрипты

- APOLLO https://github.com/mac4n6/APOLLO
- iLEAPP https://github.com/abrignoni/iLEAPP
- ArtEx https://www.doubleblak.com
- Sysdiagnose https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
- ZPET https://www.duffy.app/ZPET
- iOS Triage https://github.com/RealityNet/ios_triage

Ресурсы для экспертов

Блоги

- Checkra1n Era https://blog.digital-forensics.it
- macOS & iOS Forensic Research https://www.mac4n6.com
- D20 Forensics https://blog.d204n6.com
- Oxygen blog https://www.oxygensoftware.ru/ru/news/articles
- Elcomsoft blog https://blog.elcomsoft.ru

Ресурсы для экспертов

Полезные бесплатные программы

- plist Editor https://www.icopybot.com/plist-editor.htm
- DB Browser for SQLite https://sqlitebrowser.org
- SQLite Expert http://www.sqliteexpert.com
- 3uTools http://www.3u.com
- iMobileDevice http://docs.quamotion.mobi/docs/imobiledevice/

- **checkra1n** **https://checkra.in**

Современные методы извлечения данных из Apple iPhone

Вопросы?

(c) ElcomSoft 2020
Vladimir Katalov, ElcomSoft Co. Ltd.

http://www.elcomsoft.ru
https://blog.elcomsoft.ru

Facebook: ElcomSoft
Twitter: @elcomsoft