Acquisizione logica di dispositivi iOS: tipologie, analisi e differenze nelle modalità e nei dati estratti - parte II

Author : Luca Cadonici

Date : 16 Settembre 2020

Segue dalla prima parte

Acquisizione logica da backup iTunes

Sfruttando i backup di iTunes, l'acquisizione logica si configura come la più veloce, semplice e sicura tipologia di acquisizione. È inoltre compatibile con ogni tipologia di dispositivo iOS, richiedendo semplicemente l'installazione di iTunes e l'utilizzo di un cavo Apple, più un adattatore iBUS nel caso degli Apple Watch.

I **dati acquisibili** per tipologia e quantità sono notevoli:

- informazioni sul dispositivo;
- file multimediali;
- database SQL contenenti informazioni sui file cancellati;
- log diagnostici e di *crash;*
- dati condivisi dalle applicazioni di terze parti.

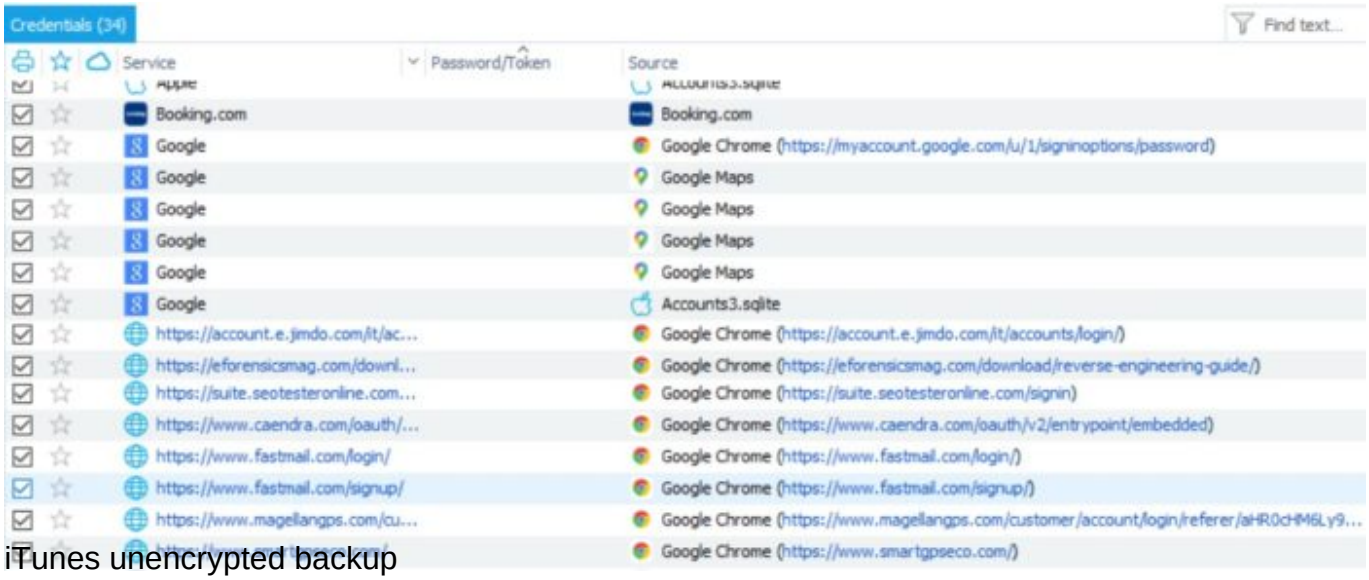
Inoltre, rispetto alla semplice analisi di un backup iTunes, l'analisi logica ci permette di acquisire **metadati** e anteprime dei file multimediali. Restano esclusi, invece, i dati non compresi nei backup di iTunes quali, ad esempio, i messaggi di posta elettronica gestiti da Google Mail.

Esistono differenze significative tra l'acquisizione di un backup protetto da password e uno non crittografato.

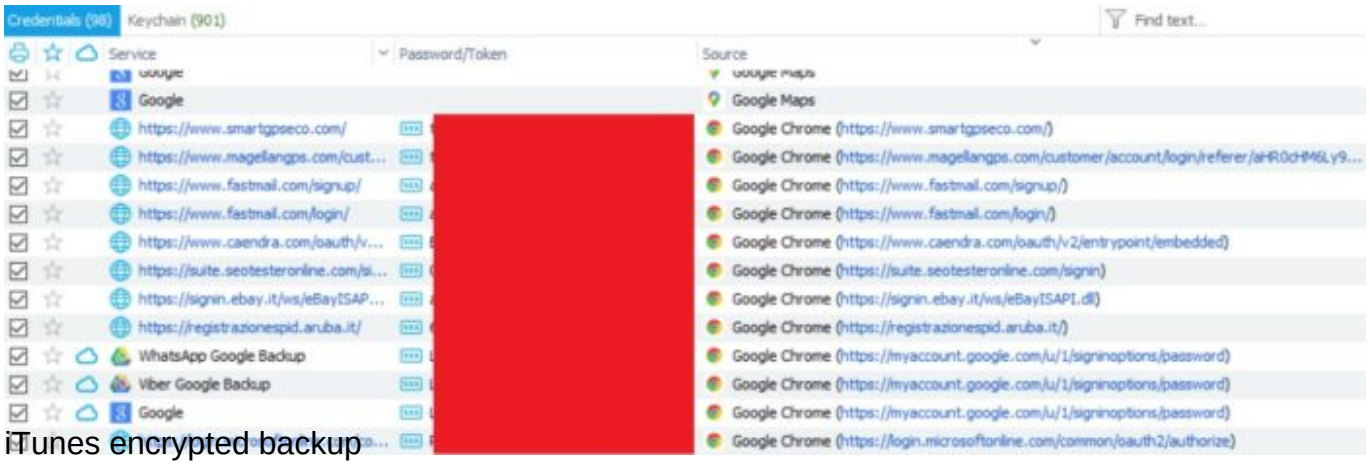
I backup cifrati infatti permettono di acquisire anche i seguenti dati:

- *keychain;*
- dati sanitari (*Health*, *Activity*);
- dati relativi alla domotica (*Homekit*);
- cronologia di navigazione e password di Safari (*bookmarks* e *web searches* sono

presenti anche nei backup non cifrati);
- registro delle chiamate completo (elenco chiamate telefoniche; le chiamate VoIP vengono memorizzate anche nel backup non crittografato);
- impostazioni Wi-Fi;
- password memorizzate nei browser web.



iTunes unencrypted backup



iTunes encrypted backup

È opportuno quindi procedere, ove possibile, alla generazione di un backup cifrato con password nota, al fine di massimizzare la quantità di dati acquisibili. Strumenti come UFED impostano automaticamente una **password convenzionale** (es.1234) al momento della creazione del backup qualora essa non sia già stata impostata sul dispositivo. Tale password infatti non coincide con il codice di sblocco, anche se spesso gli utenti tendono a confonderla. Se questo può essere un vantaggio in caso di coincidenza con il codice noto, spesso tale

password viene semplicemente dimenticata e l'utente non è in grado di produrla neanche volendo.

Sebbene sia possibile effettuare un attacco a forza bruta con tempi di sblocco incerti, le più recenti impostazioni di sicurezza Apple paradossalmente aiutano gli analisti nella modifica delle password dei backup di iTunes. Prima di iOS 11, la password dei backup di iTunes veniva richiesta al momento della configurazione del dispositivo e non era possibile cambiarla senza effettuare un *reset to factory* del dispositivo. In questo modo un backup cifrato era essenzialmente irrecuperabile, salvo l'impiego di mesi o anni per attacchi crittografici a forza bruta; per cui le uniche strade possibili erano l'impiego di *lockdown records* o il *jailbreak*. Da iOS 11 la situazione è cambiata drasticamente, lasciando la possibilità di cambiare la password di backup senza una sostanziale perdita di dati da parte dell'utente in possesso del codice di sblocco del dispositivo, come riportato dal supporto Apple[2], è possibile infatti procedere alla **rimozione della password di backup** tramite una serie di click, nell'ordine: *Settings -> General -> Reset -> Reset All Settings*, seguita dall'immissione del codice di sblocco. Terminata la seguente procedura, l'utente apprezzerà solo piccoli cambiamenti relativi allo sfondo, alla luminosità del display, alla percentuale di carica della batteria, alla regolazione della sveglia, a impostazioni e notifiche delle applicazioni; non risulteranno però rimossi nessun file o password, con l'eccezione delle password Wi-Fi che andranno invece nuovamente immesse. I dati Wi-Fi, SSID e password, sono infatti la parte più cospicua dei dati rimossi durante il ripristino ed è opportuno tenerlo a mente. Restano intatti, invece, i dati relativi al *Bluetooth*.

Effettuata la procedura di ripristino, sarà quindi possibile, con un dispositivo sostanzialmente inalterato per le parti di ordinario interesse investigativo, procedere alla generazione di un backup iTunes non cifrato o, ancor più interessante, un backup di iTunes cifrato con password di nostra scelta.

Acquisizione da backup iCloud

Utilizzando lo *storage* Cloud Apple è possibile acquisire i backup precedenti dei dispositivi ed eventualmente apprezzarne le modifiche e, ancor più importante, rilevare la presenza di dati non più presenti nel dispositivo.

Il backup di iCloud è suddiviso in blocchi caricati singolarmente in ordine casuale su uno o più server di terze parti. Ogni blocco è crittografato con una chiave di crittografia univoca e individuale senza la quale, anche se assemblati nel giusto ordine, i blocchi non possono essere decifrati. La **politica di sicurezza Apple** prevede infatti la memorizzazione dei dati Cloud cifrati su server di terze-parti quali *Amazon*, *Microsoft*, *Google*, *AT&T* e il Governo cinese, per i dati degli utenti residenti nella Cina continentale. Apple conserva però le chiavi di cifratura sui propri server nei data center di Cupertino senza, ufficialmente, passarli a terzi se non in presenza una richiesta formale delle Autorità. I dati considerati tra i più sensibili però, come ad esempio quelli relativi alla salute o i backup stessi dei dispositivi iOS, sono memorizzati con cifratura *end-to-end* tale che non sia possibile procederne alla decifratura senza la completa disponibilità del dispositivo che li ha generati. I più recenti aggiornamenti di sicurezza hanno inoltre annullato la possibilità di procedere ad acquisizione tramite token estratto dai dispositivi di interesse[3], complicando ulteriormente le cose per i software forensi, i quali presentano soluzioni varie per

portare a termine il compito, tra cui l'uso, ad esempio, di dispositivi sottoposti a *jailbreak*[4].

I backup di iCloud presentano alcune analogie con i backup di iTunes:

- stesso contenuto di un backup non crittografato di iTunes;
- suddivisione in blocchi;
- *Keychain* crittografato con una chiave basata sull'hardware.

Significativamente, Apple attribuisce ai backup iCloud lo stesso livello di sicurezza dei backup locali non cifrati, lasciando intendere che la generazione di un backup locale protetto da password resti ancora la soluzione che offre più garanzie in termini di sicurezza. Anche in questo caso Apple non fornisce alcuno strumento per lavorare direttamente con i backup di iCloud, ripristinabili comunque in nuovo dispositivo iOS tramite immissione di ID Apple e password.

Da non sottovalutare infine la possibilità di avere più backup di iCloud presenti per lo stesso dispositivo, differenza importante con i backup locali, limitati a uno per dispositivo per ogni *workstation*.

Riferimenti

M. Epifani - P. Stirparo, *Learning iOS Forensics* – Packt Publishing
https://blog.elcomsoft.com/2014/03/itunes-icloud-backups/
https://blog.elcomsoft.com/2017/11/ios-11-horror-story-the-rise-and-fall-of-ios-security/
https://support.apple.com/en-ca/guide/security/aside/sec8e00e0dd8/1/web/1
https://support.apple.com/en-us/HT204136

Note

[2]https://support.apple.com/en-us/HT205220

[3] https://blog.elcomsoft.com/2020/07/downloading-ios-13-and-ios-14-icloud-backups/

[4] *Extracting iCloud backups using an auxiliary device*, documentazione del supporto Oxygen allegato al software Oxygen Forensic Detective v. 12.6 (luglio 2020)

Articolo a cura di **Luca Cadonici**