

CONSEGUENZE E RILEVAMENTO DEL TAMPERING SUI MESSAGGI WHATSAPP

Dott. Andrea Lazzarotto

MI OCCUPO DI

- Consulenza **informatica forense**
- **Sviluppo software**, tecnologie web e applicazioni mobili
- **Reverse engineering**, con particolare interesse per le app Android
- RecuperaBit, Carbon14, CAINE

ATTENZIONE

Lo scopo di questa presentazione è di **presentare in modo discorsivo** i risultati degli esperimenti effettuati.

Alcune parti potrebbero essere caratterizzate da un **contenuto leggermente più tecnico**. Queste saranno contrassegnate dal simbolo:



WHATSAPP

- È l'applicazione di messaggistica più utilizzata in molte nazioni, in Italia ha una **penetrazione del mercato pari all'85%** (<https://lazza.me/2HE5GwU>)
- Ostacoli per l'analisi: database di backup criptati, difficoltà di accesso ai dati su telefoni non “sbloccati”, a volte si ricorre agli screenshot
- Il contenuto delle conversazioni può essere interessante:
 - *UK says WhatsApp lets paedophiles and gangsters operate beyond the law*, Reuters, Ottobre 2017 (<https://lazza.me/2Ex6Sjk>)
 - *WhatsApp admits encryption has helped criminals as it plans crackdown on illegal behaviour*, The Telegraph, Luglio 2018 (<https://lazza.me/2wjCBAAb>)



Proviamo a ragionare come dei malintenzionati... e se fosse possibile **manomettere i messaggi WhatsApp**, o crearli da zero?

Il nostro obiettivo è riuscire a farlo su uno smartphone non “sbloccato” (senza *root*) preferibilmente **senza lasciare tracce**.

ESPERIMENTI

- 1) Modifica di un messaggio esistente, **cambiandone il contenuto** a nostro vantaggio
- 2) Inserimento di **un nuovo messaggio falso** (ricevuto) all'interno di una conversazione



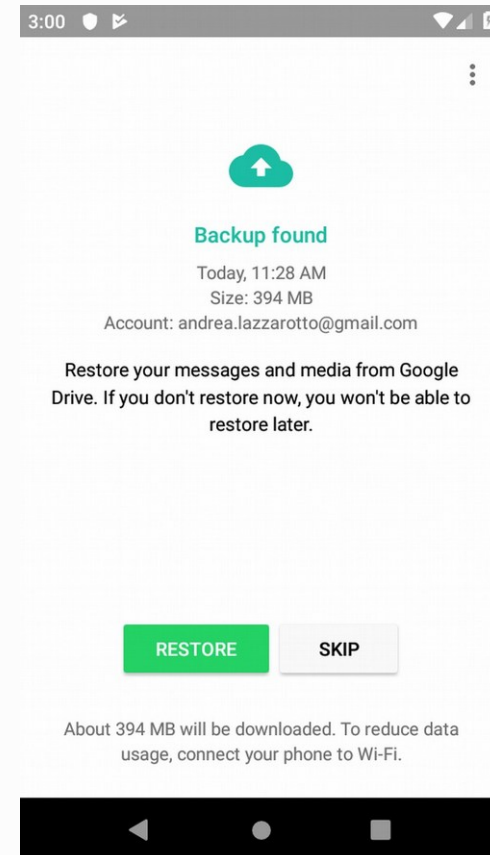
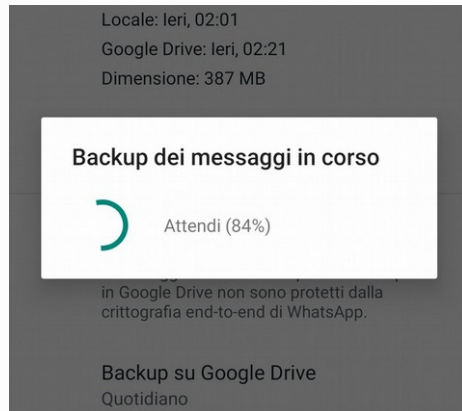
PIANO D'AZIONE

- Trasferire i messaggi dallo smartphone a un dispositivo sbloccato (con *root*) tramite **backup su account Google**
- Manomettere il contenuto del database sull'altro dispositivo
- Trasferire nuovamente i messaggi nello smartphone

Nei test è stato utilizzato l'ambiente di emulazione Genymotion, ma si può adoperare anche uno smartphone "rootato".



BACKUP E RIPRISTINO



PRIMO ESPERIMENTO: MODIFICA DI UN MESSAGGIO ESISTENTE



- Chiusura totale: *Impostazioni* → *App* → *WhatsApp* → *Forza interruzione*
- Correzione dello stato del database:

```
adb shell  
sqlite3 /data/data/com.whatsapp/msgstore.db '.schema'
```

- Copia del database dallo smartphone al computer:

```
adb pull /data/data/com.whatsapp/databases/msgstore.db
```





MODIFICA DEL MESSAGGIO

Database Structure Browse Data Edit Pragmas Execute SQL

Table: messages

_id	key_remote_id	key_from_me	key_id	status	needs_push	data
Filter	Filter	Filter	Filter	Filter	Filter	non procediamo
1 186195	39334	0	3E80E08FB93A5...	0	0	Volevo dirti che non procediamo perché il preventivo è troppo alto.

Volevo dirti che non procediamo perché il preventivo è troppo alto.

Database Structure Browse Data Edit Pragmas Execute SQL

Table: messages

_id	key_remote_id	key_from_me	key_id	status	needs_push	data
Filter	Filter	Filter	Filter	Filter	Filter	non procediamo
1 186195	39334	0	3E80E08FB93A5...	0	0	Volevo dirti che non procediamo perché il preventivo è troppo alto.

Volevo dirti che il preventivo va bene. Procediamo pure con il lavoro.

SOSTITUZIONE DEL FILE MODIFICATO

- Chiusura di WhatsApp e riparazione del database come prima (qualora fosse necessario)
- Sostituzione del database:

```
adb push msgstore.db
/data/data/com.whatsapp/databases/
```



SECONDO ESPERIMENTO: INSERIMENTO DI UN MESSAGGIO FALSO



- Partiamo dalla **duplicazione** del messaggio di prima (*id* 186195)
- La nuova riga perde la colonna *key_id* (deve essere univoca), inoltre riceve un nuovo *id* (186936)
- Dobbiamo **alterare la data di invio e ricezione** del messaggio artefatto

	_id	key_remote_jid	key_from_me	key_id	status	needs_push	
	Filter	39334	@s.whatsapp.net	Filter	Filter	Filter	Filter
1	186198	39334	@s.whatsapp.net	3EB062415070E867821A	5	0	https://www.onif.it/firenze-31-0
2	186197	39334	@s.whatsapp.net	3EB033D8700818973FDC	5	0	Ciao.
3	186196	39334	@s.whatsapp.net	3EB03FA2CDBFCA2279D6	5	0	OK d'accordo
4	186195	39334	@s.whatsapp.net	3EB0E08FB93A54E1C403	0	0	Volevo dirti che il preventivo va b
5	186194	39334	@s.whatsapp.net	3EB04045FD41A8164E51	0	0	lo tutto bene, grazie.
6	186193	39334	@s.whatsapp.net	3EB0B33F4ABEBFA4CDA5	5	0	lo bene, e tu?
7	186192	39334	@s.whatsapp.net	3EB0301EC0A54569FA3A	5	0	Ciao
8	186191	39334	@s.whatsapp.net	3EB01288F9FA668ABCA	0	0	ciao come va?
9	186190	39334	@s.whatsapp.net	D13F0807E0C7AF28591D0B09780B...	0	0	
10	186189	39334	@s.whatsapp.net	9A0086F8F787D911003ACA2DE1B5...	0	0	
11	186188	39334	@s.whatsapp.net	3EB06D36264352F187DA	5	0	
12	186187	39334	@s.whatsapp.net	CCFD1E1A182782F37E4513886C98...	0	0	
13	186186	39334	@s.whatsapp.net	015673E6D16627F9C8F8E3DC2DC5...	0	0	
14	186185	39334	@s.whatsapp.net	3EB04C33BF18AFB9881A	5	0	
15	186184	39334	@s.whatsapp.net	3EB042D92A83380479FA	5	0	
16	186057	39334	@s.whatsapp.net	963157E144C80BC6D698AB4E4E8...	5	0	
17	186056	39334	@s.whatsapp.net	43D6E9D0C8DCA068A7B0599D6DE...	0	0	
18	186055	39334	@s.whatsapp.net	2701A2872605CC4543E601595F85...	0	0	

	_id	key_remote_jid	key_from_me	key_id	status	needs_push	
	Filter	39334	@s.whatsapp.net	Filter	Filter	Filter	Filter
1	186198	39334	@s.whatsapp.net	3EB062415070E867821A	5	0	https://www.onif.it/firenze-31-0
2	186197	39334	@s.whatsapp.net	3EB033D8700818973FDC	5	0	Ciao.
3	186196	39334	@s.whatsapp.net	3EB03FA2CDBFCA2279D6	5	0	OK d'accordo
4	186195	39334	@s.whatsapp.net	3EB0E08FB93A54E1C403	0	0	Volevo dirti che il preventivo va b
5	186936	39334	@s.whatsapp.net		0	0	Volevo dirti che il preventivo va b
6	186194	39334	@s.whatsapp.net	3EB04045FD41A8164E51	0	0	lo tutto bene, grazie.
7	186193	39334	@s.whatsapp.net	3EB0B33F4ABEBFA4CDA5	5	0	lo bene, e tu?
8	186192	39334	@s.whatsapp.net	3EB0301EC0A54569FA3A	5	0	Ciao
9	186191	39334	@s.whatsapp.net	3EB01288F9FA668ABCA	0	0	
10	186190	39334	@s.whatsapp.net	D13F0807E0C7AF28591D0B09780B...	0	0	
11	186189	39334	@s.whatsapp.net	9A0086F8F787D911003ACA2DE1B5...	0	0	
12	186188	39334	@s.whatsapp.net	3EB06D36264352F187DA	5	0	
13	186187	39334	@s.whatsapp.net	CCFD1E1A182782F37E4513886C98...	0	0	
14	186186	39334	@s.whatsapp.net	015673E6D16627F9C8F8E3DC2DC5...	0	0	
15	186185	39334	@s.whatsapp.net	3EB04C33BF18AFB9881A	5	0	
16	186184	39334	@s.whatsapp.net	3EB042D92A83380479FA	5	0	
17	186057	39334	@s.whatsapp.net	963157E144C80BC6D698AB4E4E8...	5	0	
18	186056	39334	@s.whatsapp.net	43D6E9D0C8DCA068A7B0599D6DE...	0	0	

I DATI MANCANTI



- Le due colonne `timestamp` (data messaggio) e `received_timestamp` (ricezione) sono in formato **UNIX timestamp** moltiplicato per 1000
- Per la `key_id` basta un valore **esadecimale casuale**, meglio mantenere un prefisso simile a quelli già presenti

WolframAlpha computational intelligence.

1557672133.000 unix timestamp

Input interpretation:
 $1.557672133000 \times 10^9$ (Unix time)

Corresponding Gregorian time and date:
2:42:13 pm UTC | Sunday, May 12, 2019

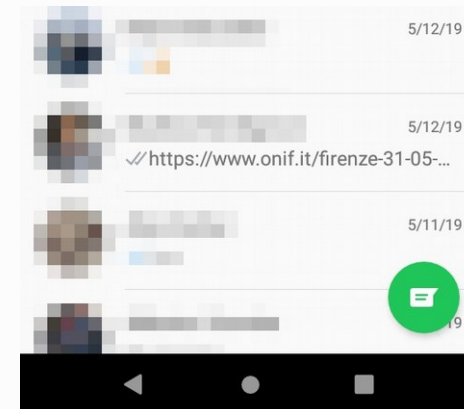
Time difference from now (7:55:04 pm UTC):

key_id	status	needs_push	
Filter	Filter	Filter	Filter
3EB062415070E867B21A	5	0	https://www.onif.it/firenze-31
3EB033D8700818973FDC	5	0	Ciao.
3EB0E08FB93A54E1C403	5	0	OK d'accordo
3EB0DF17ECAE9FAC894C	0	0	E comunque sei scarso!!! 😡
3EB0E08FB93A54E1C403	0	0	Volevo dirti che il preventivo v
3EB04045FD41A8164E51	0	0	lo tutto bene, grazie.
3EB0B33F4ABEBFA4CDA5	5	0	lo bene, e tu?
3EB0301EC0A54569FA3A	5	0	Ciao
3EB0128BF9FFA668ABCA	0	0	ciao come va?

C'È UN PROBLEMA



- Il messaggio inserito viene **visualizzato per ultimo**: significa che WhatsApp visualizza le righe ordinate per *id*
- Nell'anteprima delle chat, continua a venire mostrato il messaggio (reale) inviato per ultimo



CORREZIONE

- Incrementiamo tutti gli *id* dei messaggi successivi
- Modifichiamo i relativi riferimenti nella tabella chat

estamp	play_message_row	ast_message_row_id	_read_message_row	receipt_sent_messa	important
	1861	Filter	Filter	Filter	Filter
	186113	186113	186113	186111	1
	186198	186198	186198	186195	1

186939	186939	186939	186936
--------	--------	--------	--------



RISULTATI

- Abbiamo **modificato un messaggio** senza difficoltà. Potendo confrontare i due smartphone, si può dire che *uno dei due interlocutori ha imbrogliato...*
ma quale dei due?
- Si può **aggiungere un messaggio** finto, ma richiede più attenzione: è facile sbagliare l'ordine, inoltre si possono notare **“salti” o incongruenze** negli *id*
- In ogni caso, se le modifiche vengono effettuate con cura e attenzione, **diventa impossibile rilevarle con l'analisi del database di WhatsApp**

UN'ULTIMA COSA...

- I messaggi **sono stati trasferiti** nello smartphone originale
- L'interlocutore **non ha ricevuto la notifica** *"il codice di sicurezza di [...] è cambiato"*





Dott. Andrea Lazzarotto

<https://andrealazzarotto.com>