TelsySpywareDetector Device

Manuale utente

SOMMARIO

1. Premessa

TelsySpywareDetector[Device] è una soluzione pensata per rendere la protezione del dispositivo mobile estremamente intuitiva per l'utente finale. **Telsy**SpywareDetector[Device] permette all'utilizzatore finale, semplicemente connettendo il proprio dispositivo al Tablet tramite cavo usb, di effettuare una scansione approfondita del dispositivo senza intaccare la privacy dello stesso.

Lo scopo ultimo della soluzione è fornire uno strumento di rilevamento di Malware e/o Spyware per dispositivi mobili[1]. Il software effettua una scansione del dispositivo restituendo evidenza delle anomalie riscontrate, ove presenti nel dispositivo.

Scopo di questo documento è di descrivere la modalità di utilizzo della soluzione evidenziando:

- Gli aspetti di utilizzo legati alla scansione e diagnostica sul dispositivo tramite il Tablet;
- Le informazioni disponibili nel report sulle anomalie.
- Modalità di aggiornamento della licenza software

Figura 1. Telsy SpywareDetector[Device] componente HW Tablet con SW

[1] Per ulteriori informazioni sulle versioni smartphone compatibili con la Soluzione fare riferimento all'allegato A al presente documento.

2. Primo accesso e attivazione licenze

Accendere il Tablet e accedere all'App *TelsySpywareDetector* presente nel menu delle applicazioni.

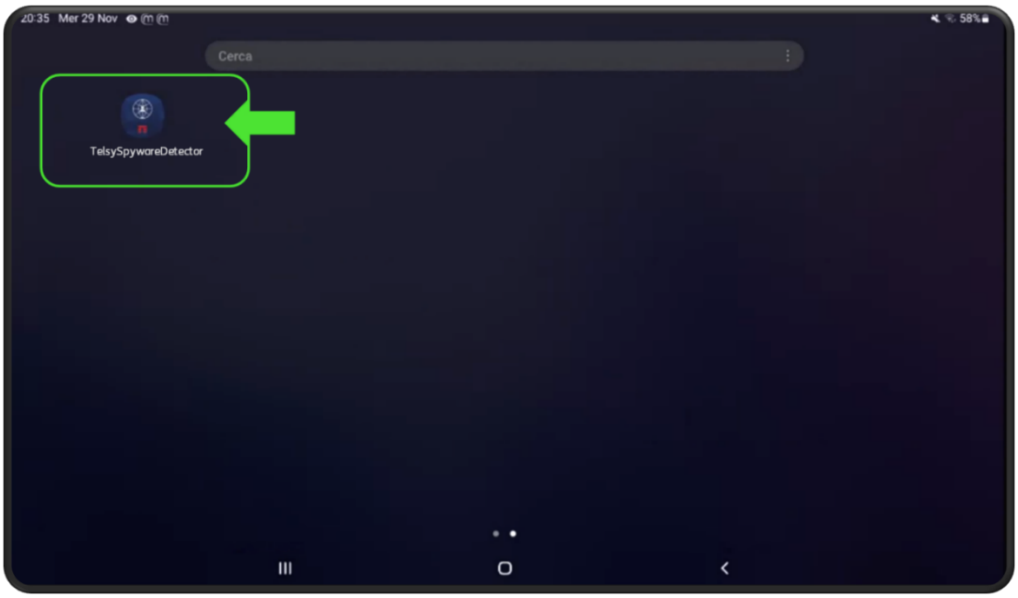

Figura 2 – App **Telsy**SpywareDetector presente nel menu delle App sul Tablet

Al primo avvio dell'applicazione sarà richiesto l'inserimento di un pin necessario all'attivazione, il quale è fornito da Telsy via mail (Welcome Letter) al momento della conferma di espletamento ordine.

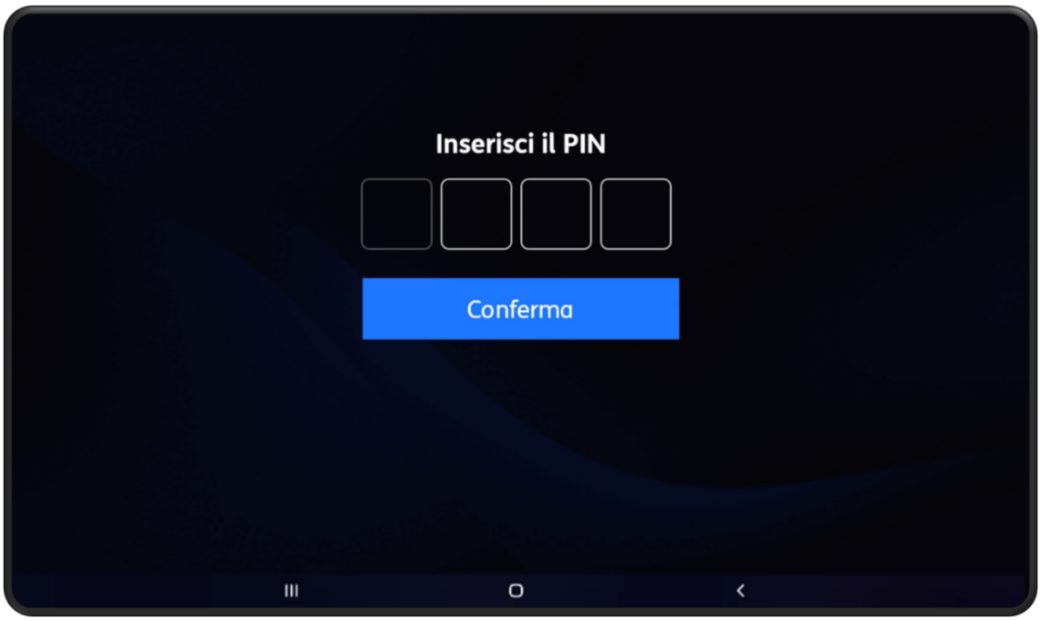

Figura 3 – Inserimento 'pin di attivazione' per il primo accesso all'App *TelsySpywareDetector*

L'attivazione delle licenze, e quindi i 12 (dodici) mesi di valenza delle licenze, decorre a partire dall'inserimento da parte del Cliente del 'pin di attivazione' richiesto al primo avvio dell'App **Telsy**SpywareDetector installata sul supporto hardware Android (Tablet).

Ad ogni connessione di un nuovo dispositivo, per il numero massimo di dispositivi previsti, uguale al numero di licenze previste nell'Offerta di cui il presente documento è allegato, il software **Telsy**SpywareDetector^{Device} estrae l'UDID del dispositivo, associandolo ad una licenza prevista, in fase di set-up, per il supporto tablet a cui il dispositivo viene connesso per la prima volta. Ove presenti più tablet nella fornitura, la sincronizzazione delle licenze avviene in modalità automatica.

Affinché l'associazione del dispositivo alla licenza avvenga con successo e sia, quindi, possibile procedere con la scansione del dispositivo è necessario che, al momento della prima connessione, il tablet sia connesso ad internet.

3. Analisi del dispositivo

L'interfaccia intuitiva del software di **Telsy**SpywareDetector^{Device} guida l'utente finale passo dopo passo nella semplice procedura di scansione del dispositivo.

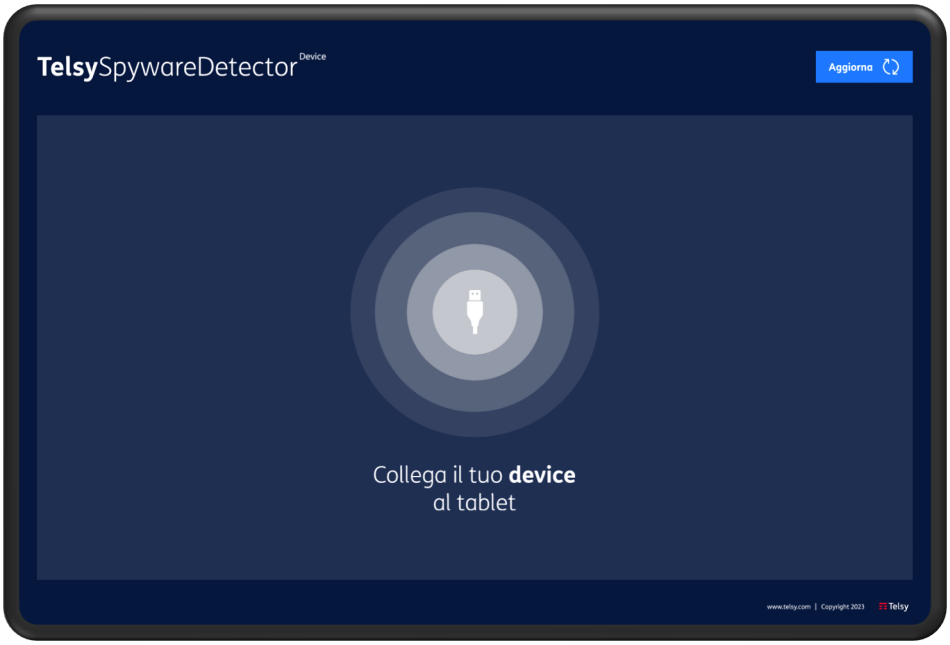

Figura 4 - Schermata iniziale che guida l'utente nella connessione del dispositivo

In caso di prima scansione del dispositivo assicurarsi che il tablet sia connesso ad una rete wifi. Procedere alla scansione seguendo le istruzioni relative al tipo di dispositivo e di sistema operativo da scansionare.

3.1. Dispositivi Samsung Android

Procedere all'attivazione della modalità sviluppatore seguendo i passaggi elencati:

- Aprire le Impostazioni del dispositivo che si intende scansionare
- Scorrere il menu principale fino in fondo e cliccare su "*Informazione sul telefono*"
- All'interno della sezione del punto precedente, andare su "Informazioni software"
- Fare Tap tante volte (circa 8) su "*Versione build*" fin quando non appare il messaggio "*Modalità sviluppatore abilitato*", se richiesto inserire il pin del dispositivo

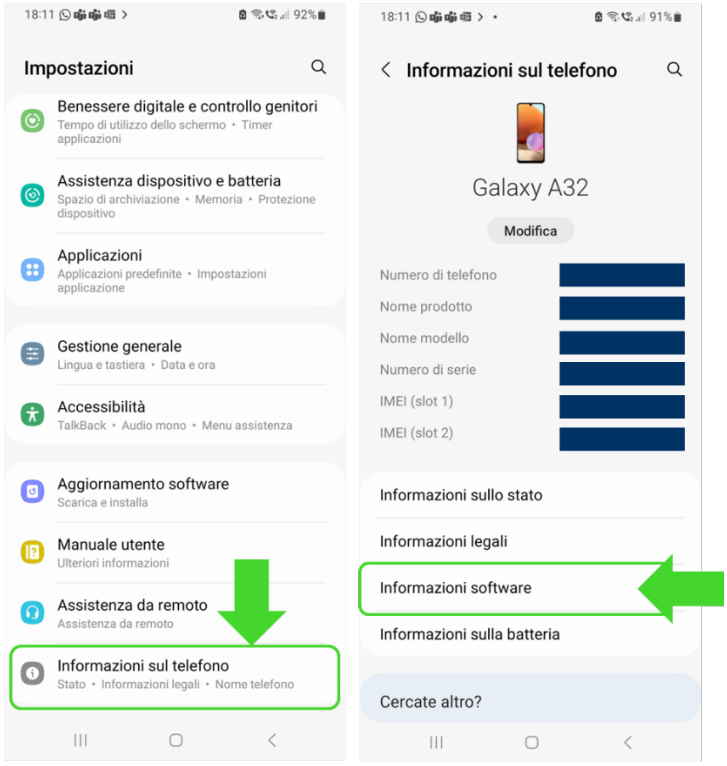

Figura 5 – Menu 'Impostazioni' e selezione '*Informazione sul telefono*'→'*Informazioni software*'

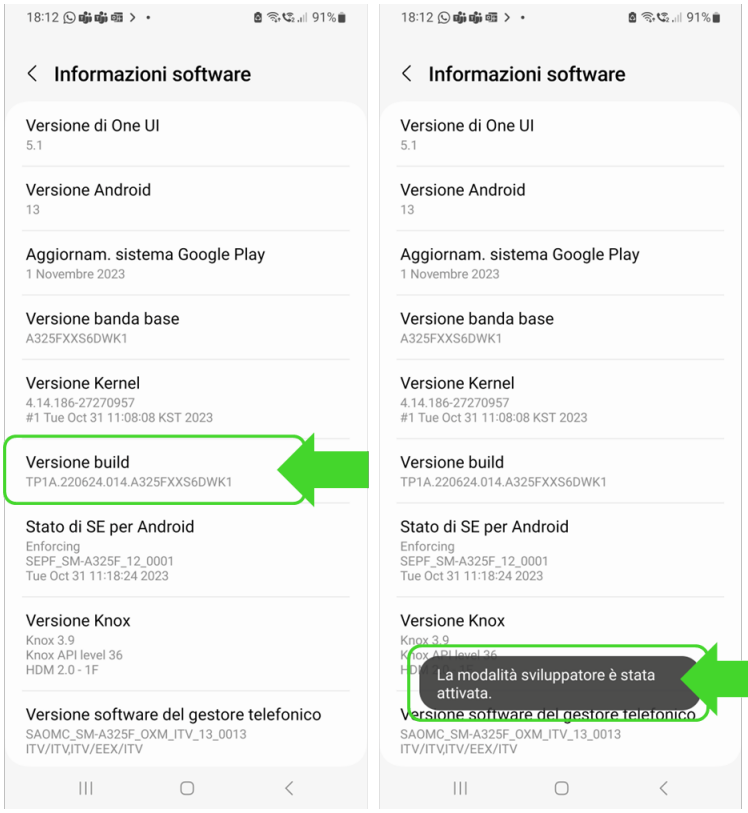

Figura 6 – Tap su '*Versione build*' per attivazione '*Modalità sviluppatore*'

Attivata la modalità sviluppatore, andare nella sezione "*Opzioni sviluppatore*" in fondo al menu principale e attivare "*Debug USB*" e confermare per abilitare la connessione del tablet al pc tramite usb.

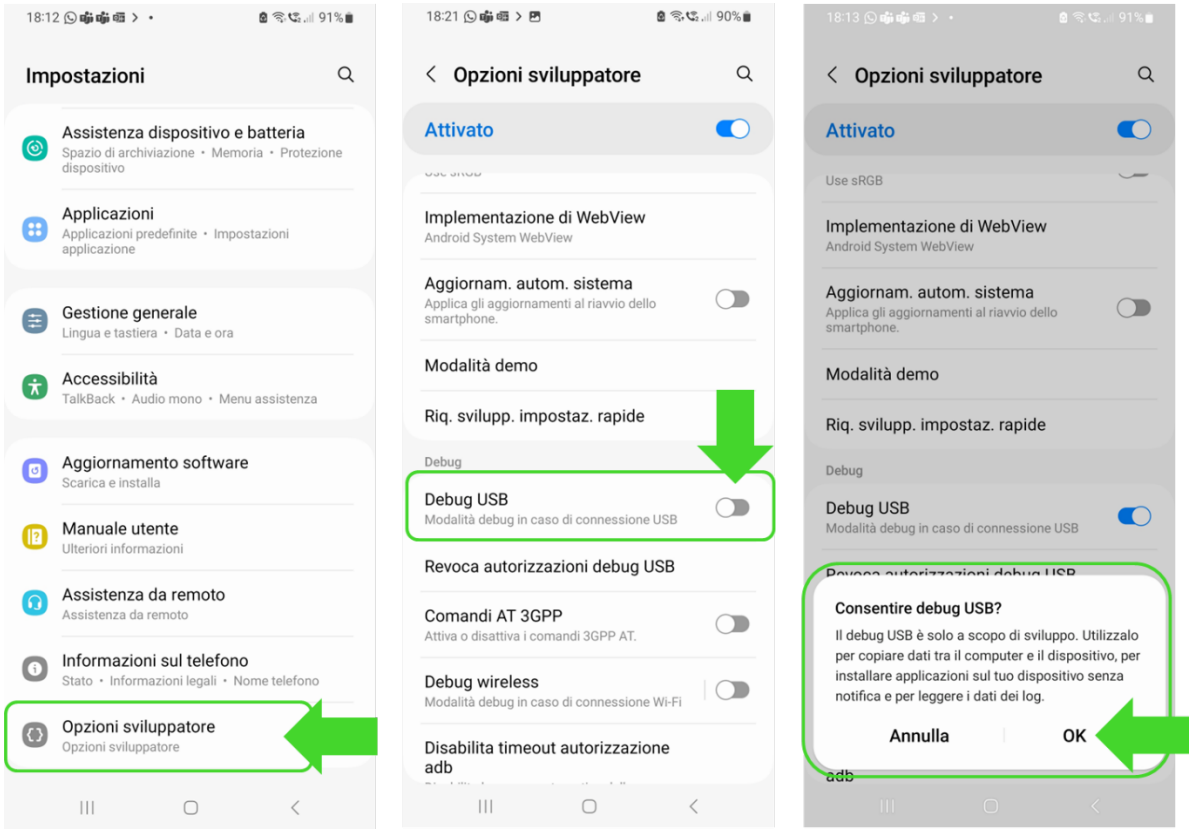

Figura 7 – Attivazione '*Debug USB*'

Collegare il dispositivo mobile al Tablet tramite cavo usb e procedere alla scansione come indicato al paragrafo 3.3. '*Avvio scansione*'

3.2. Dispositivi Apple iOS

Collegare il dispositivo mobile al Tablet tramite cavo usb.

In caso di prima scansione, una volta collegato il dispositivo al Tablet, quest'ultimo richiederà l'autorizzazione e l'abilitazione della "Modalità sviluppatore" direttamente sul dispositivo mobile dell'utente finale.

In base alla versione del sistema operativo installato sul dispositivo da scansionare, il software agirà in modalità differenti, in particolare:

- Se la versione del sistema operativo è **inferiore ad iOS 16**, il sistema richiederà una sola volta di abilitare la "Modalità sviluppatore" di cui sopra, tramite un pop-up sul device da analizzare;

Figura 8 - Pop-up di richiesta autorizzazione alla “Modalità sviluppatore" per versioni del sistema operativo inferiori ad iOS 16

- Se la versione del sistema operativo è **superiore o uguale ad iOS 16 (fino a iOS 16.7.4)**, per abilitare la “Modalità sviluppatore”, in seguito al passaggio di cui al punto 1) e rappresentato in Figura 8., è necessario spuntare la relativa casella seguendo il percorso **Impostazioni** → **Privacy e sicurezza** → **Modalità sviluppatore**, come illustrato in Figure 9 e 10.

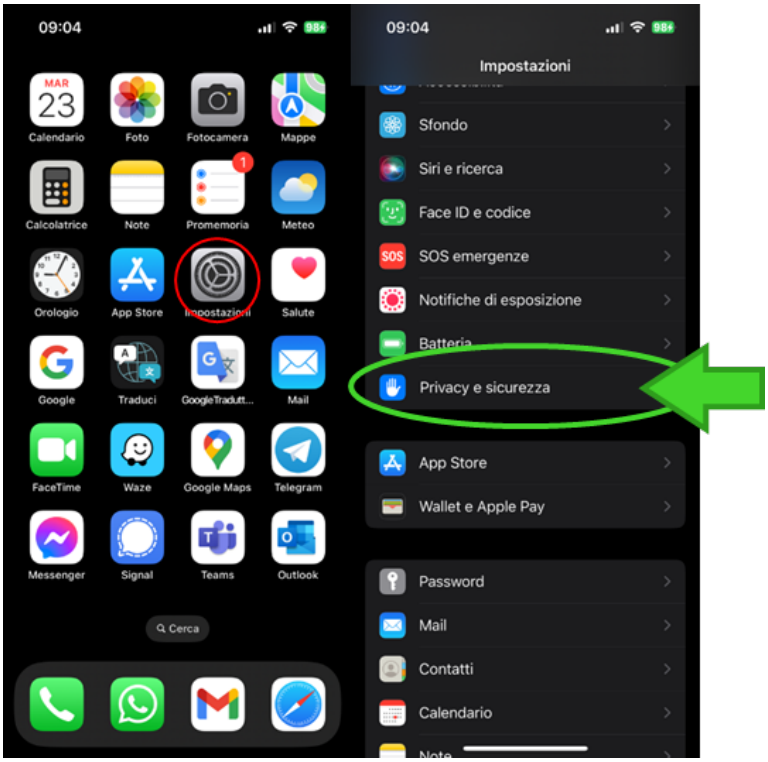

Figura 9 - Per versioni superiori o uguali ad iOS 16, per abilitare la modalità sviluppatore selezionare Impostazioni e successivamente Privacy e Sicurezza

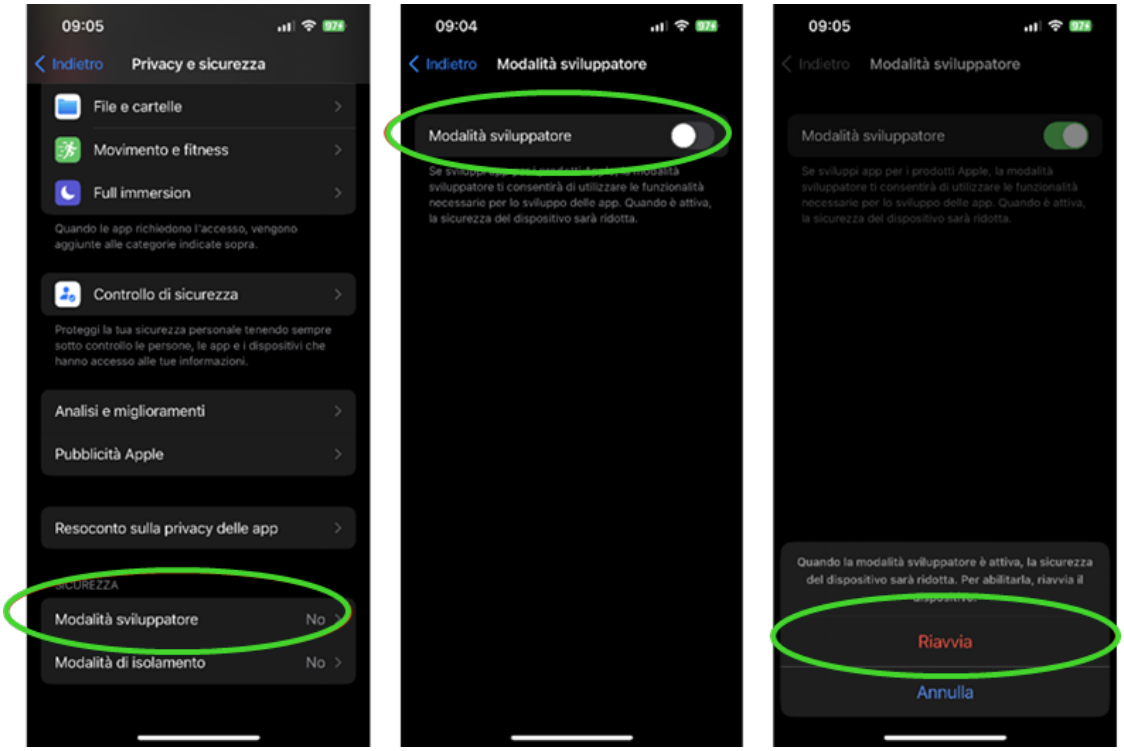

Figura 10 - In Privacy e Sicurezza, selezionare Modalità sviluppatore e abilitare la modalità. Il sistema successivamente chiede di riavviare il dispositivo

Una volta attivata la modalità sviluppatore, il dispositivo richiederà il riavvio. È necessario acconsentire al riavvio per permettere al sistema di applicare questa configurazione.
All'accensione del dispositivo dopo il riavvio, lo smartphone chiederà nuovamente la conferma di attivazione della "Modalità sviluppatore"; sarà necessario selezionare 'Attiva' sul pop-up mostrato a schermo e inserire il codice PIN di sblocco dello smartphone.

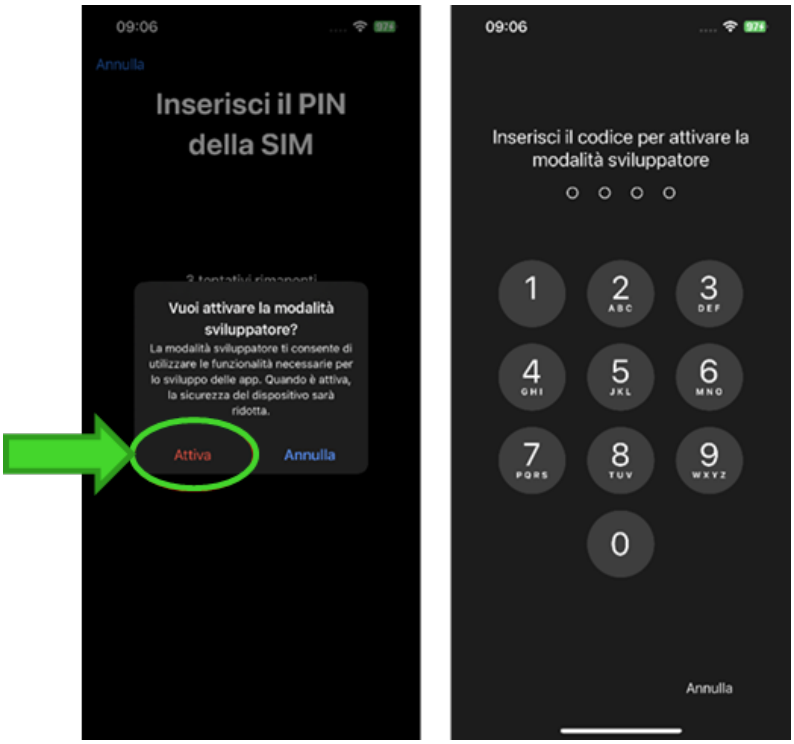

Figura 11 - Al riavvio, conferma di attivazione 'Modalità Sviluppatore' tramite pop-up e inserimento del proprio codice PIN di sblocco

È inoltre possibile verificare che la "Modalità sviluppatore" sia abilitata ri-accedendo ad **Impostazioni → Privacy e Sicurezza**, come esplicitato in Figura 12, e visualizzando "Si" alla voce "Modalità sviluppatore".

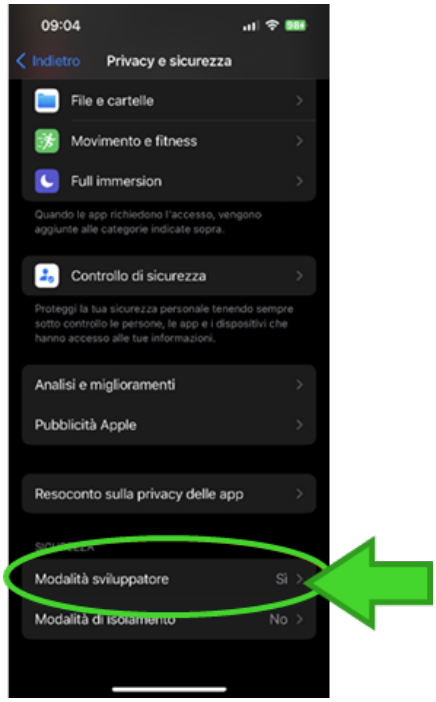

Figura 12 - Verifica di "Modalità sviluppatore" attivata

3.3. Avvio scansione

Abilitata la modalità sviluppatore sul dispositivo da scansionare, **Telsy**SpywareDetector[Device] è quindi pronto per effettuare la diagnostica. A schermo comparirà la richiesta '*Consentire all'app TelsySpywareDetector di accedere a SAMSUNG_Android/iPhone?*', flaggare '*Apri sempre TelsySpywareDetector quando si collega SAMSUNG_Android*' e cliccare su 'OK'. (Figura 13)

Se richiesto selezionare l'applicazione TelsySpywareDetector e fare doppio tap (Figura 14)

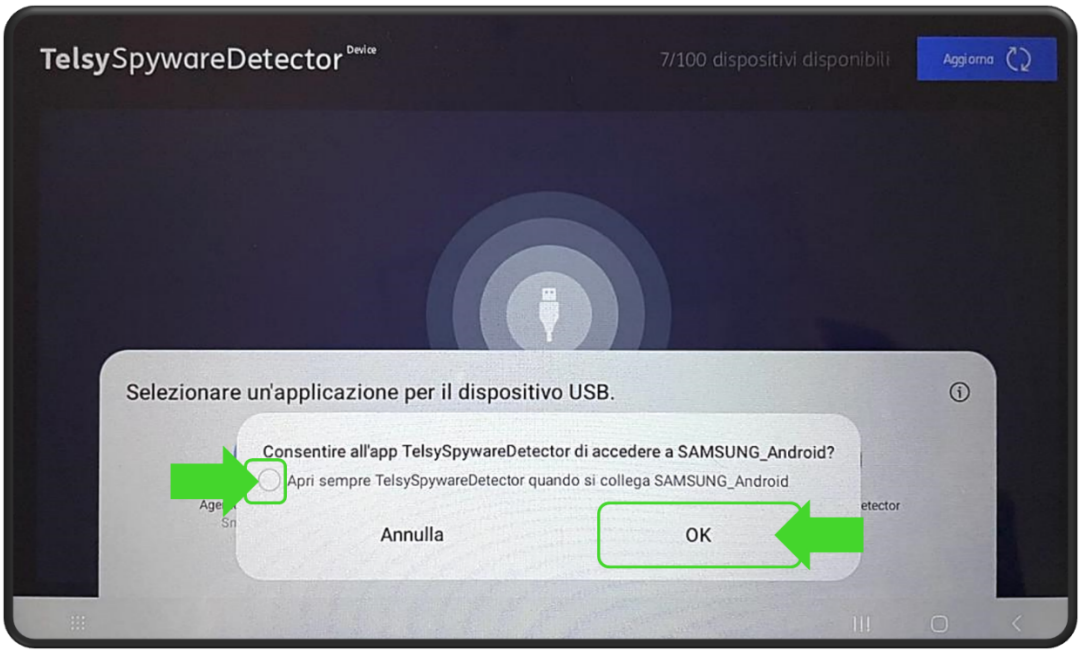

Figura 13 – Consenso di accesso al dispositivo

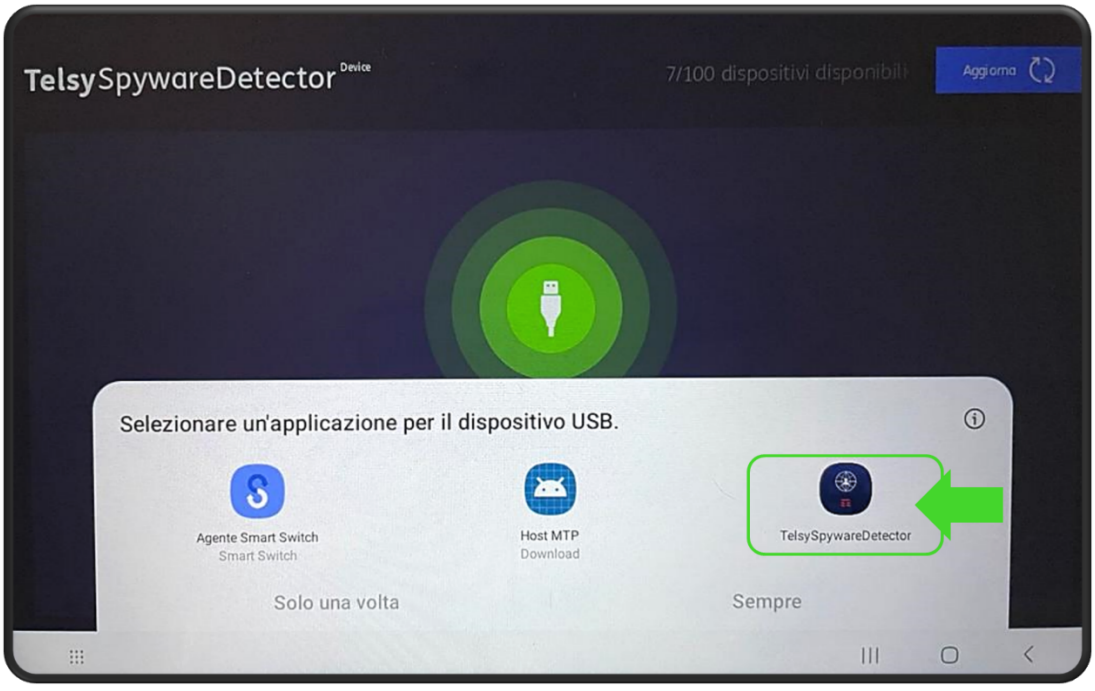

Figura 14 – Selezione app 'TelsySpywareDetector'

A questo punto il software riconosce il dispositivo connesso e tramite un intuitivo pulsante "play" invita l'utente a iniziare la scansione. (Figura 15).

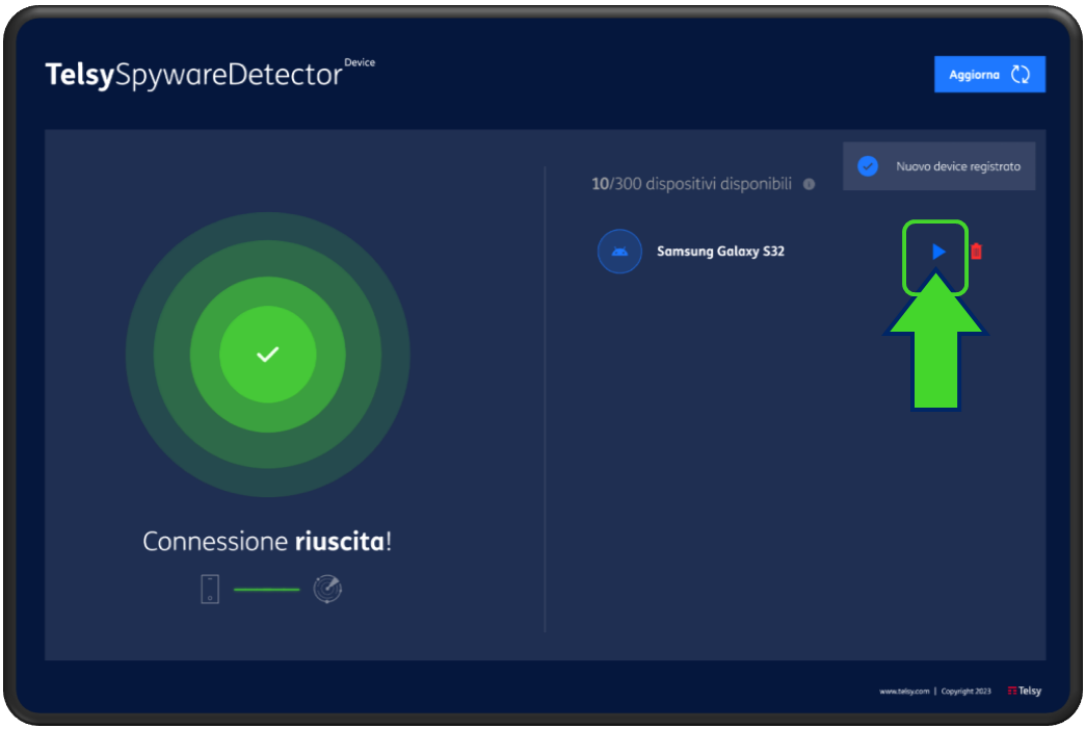

Figura 15 - Schermata iniziale per guidare l'utente nella fase di diagnostica

La fase di diagnostica ha una durata media di circa due minuti. Al termine della scansione, il sistema restituisce evidenze delle analisi effettuate e di eventuali anomalie riscontrate sul dispositivo direttamene nella dashboard e permette di ripetere l'analisi, di visualizzare il report di dettaglio ed eventualmente, di cancellarlo.

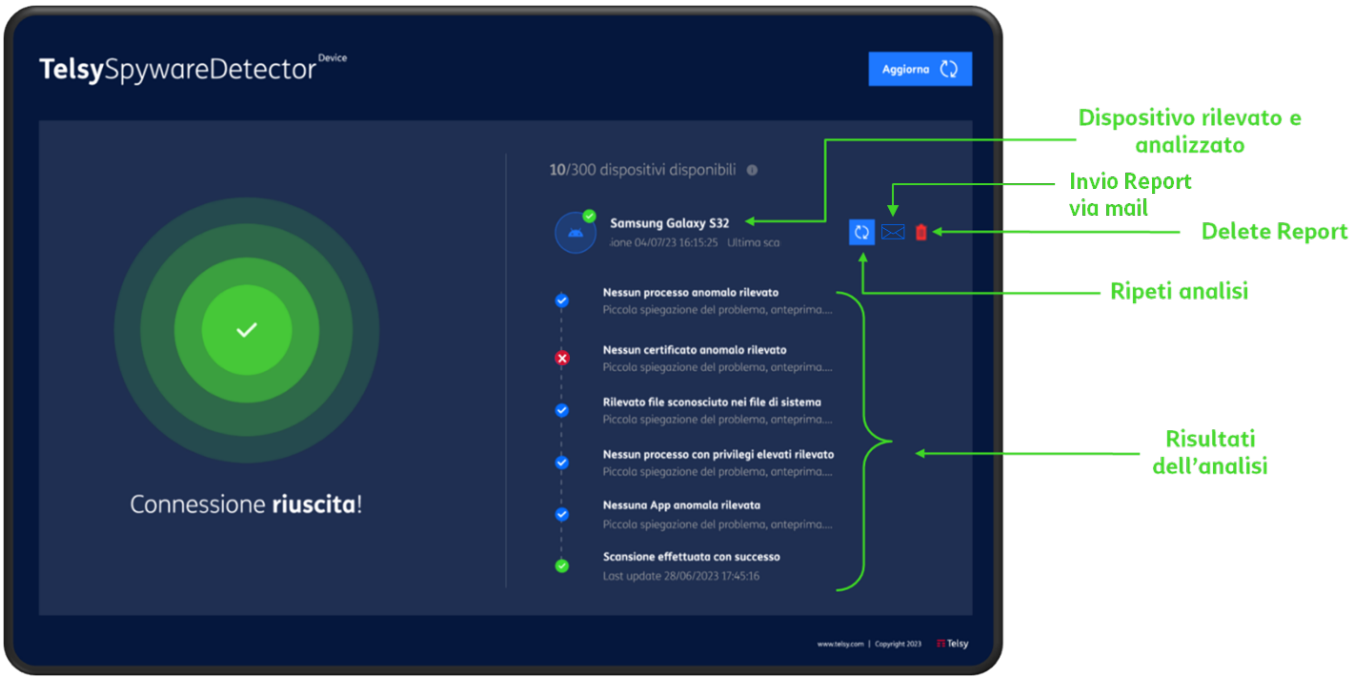

Figura 16 - Schermata post scansione del dispositivo con evidenze dell'analisi effettuata ed eventuali anomalie riscontrate.

In caso di errore di riconoscimento del dispositivo verrà mostrato a schermo un messaggio di errore, In tal caso sarà sufficiente scollegare e ricollegare il dispositivo e ripetere la procedura descritta.

4. Report delle anomalie e approfondimenti analisi

Al termine della scansione, la piattaforma di **Telsy**SpywareDetector[Device] genera un r**eport dettagliato** con tutte le **anomalie riscontrate**, e nel dettaglio:

✓	Indica che per quella porzione di analisi non è stata evidenziato alcuna anomalia
✗	Indica che è stata rilevata una anomalia
✓	Indica che l'intero processo di analisi è stato correttamente concluso

Tramite il report generato (condivisibile tramite mail direttamente d'applicazione) il personale deputato internamente all'organizzazione potrà effettuare attività di remediation necessarie per l'eradicamento della minaccia, ove applicabili, eventualmente richiedendo il supporto da remoto da parte di analisti esperti di Cyber Security di Telsy. Se incluso nell'offerta sottoscritta, il servizio di

consulenza specialistica per l'attività di remediation delle anomalie riscontrate sui dispositivi scansionati potrà essere richiesto contattando l'Help Desk dedicato.

5. Aggiornamento licenza software

In caso di variazioni dell'offerta (ad es. del numero massimo di dispositivi scansionabili) o rinnovo contrattuale sarà opportuno procedere all'aggiornamento della licenza software associata al tablet. Per procedere all'aggiornamento è sufficiente aprire l'applicazione e cliccare sul tasto 'Aggiorna' presente in alto a destra della schermata dell'app, come illustrato nell'immagine di seguito riportata (Figura 17).

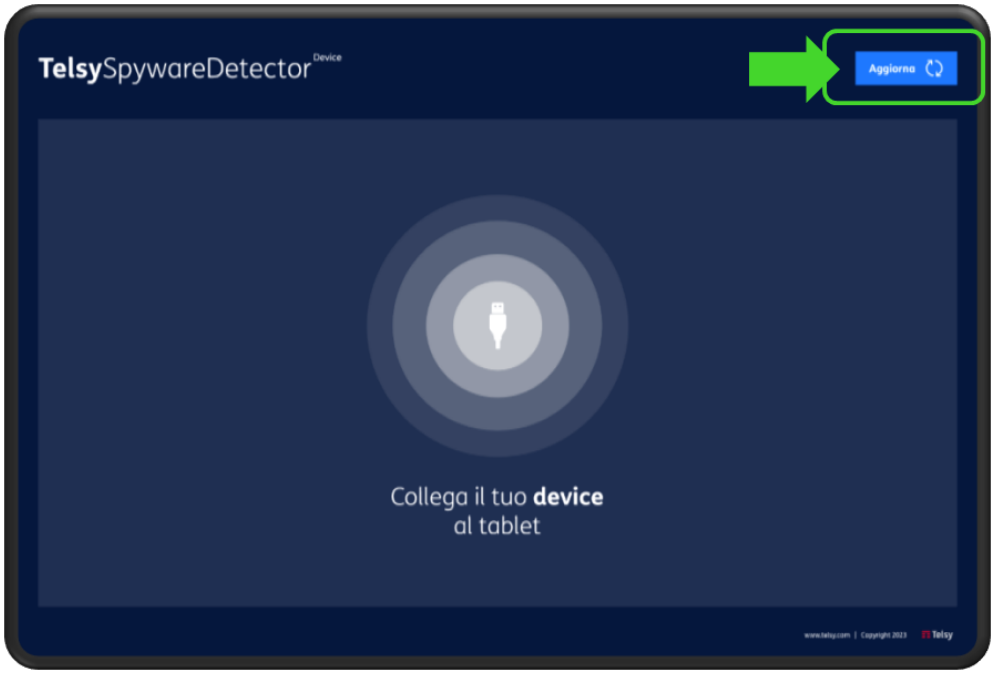

Figura 17 – Aggiornamento licenza

ALLEGATO A. DISPOSITIVI E SISTEMI OPERATIVI SUPPORTATI DAL SOFTWARE DI SCANSIONE

Di seguito vengono elencati i modelli di dispositivi con relative versioni minime e massime dei sistemi operativi supportate dal software di scansione **Telsy**SpywareDetector[Device].

La tabella sottostante verrà aggiornata contestualmente al rilascio degli aggiornamenti di OS supportati.

Brand	Model	Min Version	Max Version
Apple	iPhone 14 Pro Max	16.0.0	16.7.4
Apple	iPhone 14 Pro	16.0.0	16.7.4
Apple	iPhone 14 Plus	16.0.0	16.7.4
Apple	iPhone 14	16.0.0	16.7.4
Apple	iPhone SE 2022	15.4.1	16.7.4
Apple	iPhone 13	15.0.0	16.7.4
Apple	iPhone 13 Mini	15.0.0	16.7.4
Apple	iPhone 13 Pro Max	15.0.0	16.7.4
Apple	iPhone 13 Pro	15.0.0	16.7.4
Apple	iPhone 12	13.4.1	16.7.4
Apple	iPhone 12 Pro	13.4.1	16.7.4
Apple	iPhone 12 Mini	13.4.1	16.7.4
Apple	iPhone SE 2020	13.4.1	16.7.4
Apple	iPhone 11	13.0.0	16.7.4
Apple	iPhone 11 Pro	13.0.0	16.7.4
Apple	iPhone 11 Pro Max	13.0.0	16.7.4
Apple	iPhone XR	12.0.0	16.7.4
Apple	iPhone XS Max	12.0.0	16.7.4
Apple	iPhone XS	12.0.0	16.7.4
Apple	iPhone X GSM	11.3.1	16.7.4
Apple	iPhone 8 Plus	11.3.1	16.7.4
Apple	iPhone 8	11.3.1	16.7.4
Apple	iPhone X Global	11.3.1	16.7.4

Brand	Model	Min Version	Max Version
Samsung	Galaxy S8+/ S8	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S9/ S9+	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S10 / S10 Lite / S10e / Galaxy S10+ / S10 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S20/ S20 FE / S20 5G/ S20 5G UW/ S20+/ S20+ 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S20 Ultra/ S20 Ultra 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S21 FE 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy S22 5G / S22 Ultra 5G / S22+ 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy S23 FE	Android 13 64bit	Android 14 64bit
Samsung	Galaxy S23 Ultra	Android 13 64bit	Android 14 64bit
Samsung	Galaxy S23	Android 13 64bit	Android 14 64bit
Samsung	Galaxy S23+	Android 13 64bit	Android 14 64bit
Samsung	Galaxy Note 8	Android 11 64bit	Android 14 64bit
Samsung	Galaxy Note 9	Android 12 64bit	Android 14 64bit
Samsung	Galaxy Note 10/ Note 10 5G/ Note 10+/ Note 10+ 5G/ Note 10 Lite	Android 13 64bit	Android 14 64bit
Samsung	Galaxy A03 / A03s	Android 11 64bit	Android 14 64bit
Samsung	Galaxy A04 / A04e / A04s	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A05 / A05s	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A13 / A13 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A14 / A14 5G	Android 13 64bit	Android 14 64bit
Samsung	Galaxy A23 / A23 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A24 4G	Android 13 64bit	Android 14 64bit
Samsung	Galaxy A33 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A52s 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy A53 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy A73 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy F13	Android 12 64bit	Android 14 64bit
Samsung	Galaxy F22	Android 11 64bit	Android 14 64bit
Samsung	Galaxy F23	Android 12 64bit	Android 14 64bit
Samsung	Galaxy M13 / M13 5G	Android 12 64bit	Android 14 64bit
Samsung	Galaxy M23	Android 12 64bit	Android 14 64bit
Samsung	Galaxy M32 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy M33	Android 12 64bit	Android 14 64bit
Samsung	Galaxy M52 5G	Android 11 64bit	Android 14 64bit
Samsung	Galaxy M53	Android 12 64bit	Android 14 64bit
Samsung	Galaxy M54	Android 13 64bit	Android 14 64bit
Samsung	Galaxy Z Flip / Z Flip3 / Z Flip4 / Z Flip5	Android 13 64bit	Android 14 64bit
Samsung	Galaxy Fold/ Fold 5G / Z Fold3 5G / Z Fold4 / Z Fold5	Android 13 64bit	Android 14 64bit