kaspersky BRING ON THE FUTURE

Che cos'è lo stalkerware?

Il termine stalkerware è utilizzato per descrivere gli strumenti – programmi software, applicazioni e servizi – che consentono di spiare un'altra persona attraverso il suo dispositivo mobile. Lo stalkerware consente all'autore del reato di monitorare a distanza il dispositivo, ovvero le ricerche su Internet, la posizione, i messaggi di testo, le foto, le chiamate vocali e altro ancora. Questi programmi vengono eseguiti di nascosto in background, senza che la persona interessata ne sia a conoscenza o abbia dato il proprio consenso.

Lo stalkerware è un esempio di come le tecnologie possano essere utilizzate impropriamente per compiere abusi come ad esempio la sorveglianza della o del partner, la violenza domestica e di genere o le molestie. Nonostante lo stalkerware sia disponibile online senza limitazioni, l'autore dell'abuso è responsabile del suo utilizzo e quindi della commissione di questo reato.

Lo stalkerware ha smesso da tempo di essere una minaccia che colpisce un ridotto numero di utenti. Nel 2021 Kaspersky ha, infatti, rilevato 32.694 persone colpite da stalkerware in tutto il mondo, di cui 611 in Italia.

I principali segnali di una compromissione stalkerware

Link utili:

Coalition against Stalkerware:
https://stopstalkerware.org/it/

TinyCheck:
www.tiny-check.com

TinyCheck su github:
https://github.com/KasperskyLab/TinyCheck

Kaspersky Anti-Virus:
https://www.kaspersky.it/antivirus

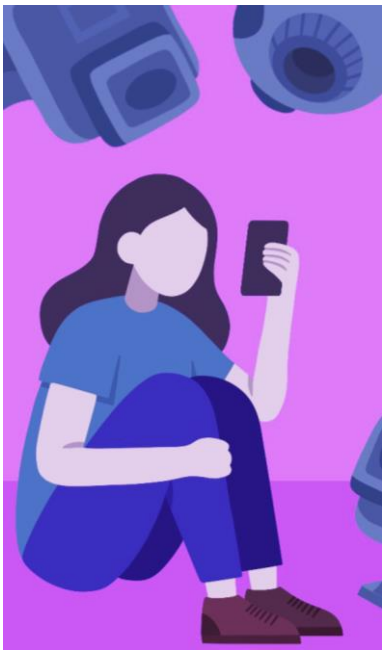
Kaspersky Internet Security:
https://www.kaspersky.it/internet-security

Kaspersky Total Security:
https://www.kaspersky.it/total-security

Kaspersky Internet Security for Android:
https://www.kaspersky.it/android-security

- **Aumento del consumo di dati:** le app spia devono accedere a Internet per trasmettere i dati da monitorare o inviarli all'autore del reato. Un aumento inspiegabile del loro consumo può indicare un'infezione da stalkerware.
- **Minor durata della batteria e rallentamento dei processi:** a causa delle attività in background, lo stalkerware consuma molta memoria, CPU e batteria, rallentando le prestazioni dello smartphone. Pertanto, tutti i processi e le app in esecuzione devono essere controllati regolarmente.
- **App sconosciute non installate dall'utente:** è importante fare attenzione alle applicazioni che non si ricorda di aver scaricato per escludere la possibilità che sia stato installato un software di monitoraggio senza consenso.
- **Conoscenza dettagliata inspiegabile di terzi:** se persone non autorizzate sono a conoscenza di foto scattate di recente, luoghi visitati o altre informazioni personali custoditi all'interno di account o dispositivi protetti da password, il sospetto che il proprio dispositivo possa essere affetto da stalkerware è evidente.

Rilevare lo stalkerware con TinyCheck



Da anni Kaspersky si batte attivamente contro lo stalkerware ed è tra i fondatori della Coalition Against Stalkerware. Per rilevare un'infezione da stalkerware senza segnalarla al responsabile, gli esperti di cybersecurity hanno sviluppato uno strumento open-source TinyCheck, che può essere utilizzato da ONG e forze di polizia per aiutare le persone affette da stalking digitale. Opera su un dispositivo separato dallo smartphone, Android o iOS, che è sorvegliato.

TinyCheck è uno strumento di sicurezza che non legge il contenuto delle conversazioni (come SMS o e-mail) ma interagisce solo con i server/IP online con cui lo smartphone comunica. TinyCheck quindi non è in grado di sapere con chi o di cosa una persona stia parlando. Il registro di rete del dispositivo analizzato non viene condiviso; né Kaspersky né terzi ricevono questi dati. Tutte le analisi sono eseguite a livello locale.

Per ulteriori informazioni consultare www.tiny-check.com.

Consigli di Kaspersky per le persone colpite da stalkerware

- Se l'autore del reato si rende conto che lo stalkerware o qualsiasi altro programma di monitoraggio è stato rimosso o modificato, potrebbe peggiorare la situazione. Pertanto, lo stalkerware può essere rimosso solo se si può escludere un ulteriore pericolo per la vittima, dopo aver messo in sicurezza eventuali prove e aver capito come tutelarsi al meglio.
- Contattare centri dedicati e punti di assistenza come Donne in Rete contro la violenza (D.i.Re) per ricevere un supporto professionale specifico.
- Fare riferimento alla Polizia Postale e delle Comunicazioni per eventuali segnalazioni online, richieste di informazioni o contatto telefonico, anche in anonimato.
- Il sito della Coalition Against Stalkerware offre assistenza iniziale. Un video esplicativo disponibile su questo sito permette di riconoscere i segnali di un eventuale stalkerware, raccomandando ulteriori misure e comportamenti da adottare o evitare.

Come proteggersi dallo stalkerware sui dispositivi mobili

- Controllare le autorizzazioni delle app installate: le applicazioni stalkerware possono essere camuffate con un nome falso. Eliminare le app che si usano raramente o mai.
- Verificare le impostazioni di download da "fonti sconosciute" sui dispositivi Android: devono essere disattivate.
- Controllare la cronologia di navigazione personale: per scaricare lo stalkerware, l'autore deve visitare siti web che la persona colpita probabilmente non conosce. Potrebbe non esserci alcuna cronologia se l'autore del reato l'ha cancellata.
- Utilizzare una soluzione di sicurezza informatica affidabile come Kaspersky Anti-Virus, che protegge da tutti i tipi di minacce mobili e effettua regolarmente una scansione del dispositivo.