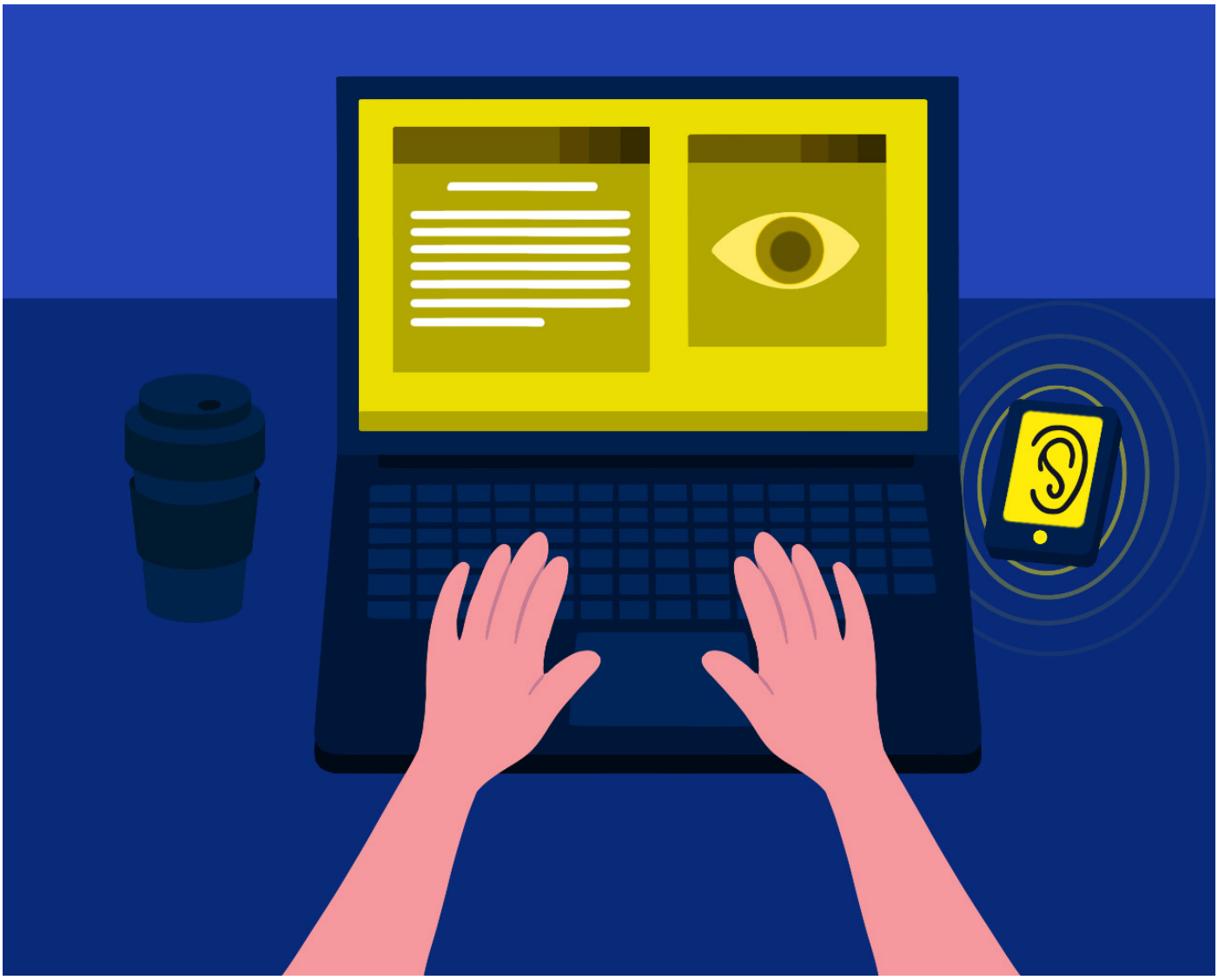


Lo stato dello **stalkerware** nel 2021

COALITION AGAINST STALKERWARE

kaspersky

Contenuto

Principali osservazioni 2021

Ogni anno Kaspersky analizza l'uso dello stalkerware nel mondo per meglio comprendere le minacce che ciò comporta. Lavoriamo con stakeholder sia del settore pubblico che privato per sensibilizzare le persone e per trovare soluzioni che permettano di affrontare al meglio questo importante problema.

Lo stalkerware permette di spiare in segreto la vita privata di altre persone attraverso i dispositivi smart e viene spesso utilizzato per facilitare la violenza psicologia e fisica nei confronti di un partner intimo. Il software, disponibile in commercio, è in grado di accedere a una serie di dati personali, tra cui localizzazione del dispositivo, cronologia del browser, messaggi di testo, chat sui social media, foto e altro. La commercializzazione dello stalkerware non è illegale, ma lo è il suo uso senza il consenso della vittima. I perpetratori sfruttano questo incerto quadro normativo tuttora in vigore in molti paesi. Lo stalkerware costituisce una violazione della privacy e una forma di abuso compiuto con l'ausilio della tecnologia. Per affrontare questa complessa minaccia in modo esaustivo, al fine di supportare al meglio vittime e sopravvissuti, servono strumenti innovativi da un punto di vista legislativo, sociale e tecnologico.

Dati in evidenza 2021

- **I dati Kaspersky mostrano che nel 2021 sono stati 32.694 gli utenti colpiti dallo stalkerware a livello globale.** Questi dati sono in calo rispetto ai numeri del 2020 e rappresentano un minimo storico da quando abbiamo raccolto per la prima volta i dati sullo stalkerware nel 2018. Questo potrebbe sembrare un motivo per rallegrarsi, ma non lo è.
- **La cyber-violenza è in crescita,** soprattutto da quando è iniziata la pandemia. Con le persone costrette a socializzare sempre meno e a trascorrere più tempo in casa, i perpetratori si sono sentiti più al sicuro, e questo probabilmente li ha resi meno disposti ad installare uno stalkerware per spiare il proprio partner. Purtroppo gli autori di abusi hanno a loro disposizione un'ampia gamma di strumenti, nella forma di dispositivi smart, per spiare o stalkerare le loro vittime. Le organizzazioni no-profit con cui Kaspersky opera in stretta collaborazione hanno condiviso simili osservazioni dopo aver lavorato con perpetratori e vittime di stakerware. È importante ricordare che questi numeri includono solo utenti Kaspersky: non prendono in considerazione gli utenti che utilizzano le soluzioni di sicurezza IT dei nostri concorrenti o coloro che non hanno nessuna soluzione di sicurezza informatica installata sui loro dispositivi mobili. Dunque si vede solo la punta dell'iceberg: se da un lato è

difficile calcolare il numero esatto di utenti colpiti nel mondo, membri della Coalition against Stalkerware (Coalizione contro gli stalkerware) stimano che la cifra potrebbe essere almeno di 30 volte più alta, arrivando a un numero vicino a 1 milione di vittime in tutto il mondo, ogni anno.

- Sulla base dei dati ottenuti dalla Kaspersky Security Network, **Russia, Brasile e Stati Uniti rimangono i paesi più colpiti.** Questo è in linea con le statistiche degli ultimi due anni. A livello regionale, i numeri più elevati di utenti colpiti si riscontrano in:
  - Germania, Italia e Regno Unito (Europa)
  - Turchia, Egitto e Arabia Saudita (Medio Oriente e Africa)
  - India, Indonesia e Vietnam (Asia-Pacifico)
  - Brasile, Messico e Colombia (America Latina)
  - Stati Uniti (Nordamerica)
  - Federazione Russa, Ucraina e Kazakistan (Europa orientale (esclusi i paesi dell›UE), Russia and Asia centrale)
- **Cerberus e Reptilicus sono risultate le applicazioni stalkerware più utilizzate,** con 5.575 e 4.417 utenti colpiti, rispettivamente, a livello globale.

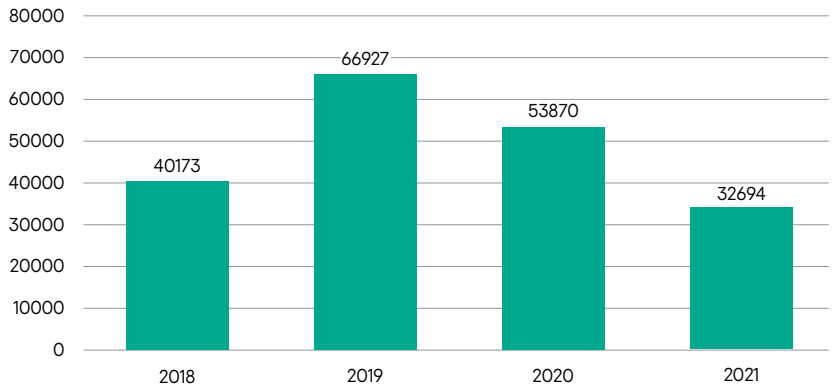
Trend osservati da Kaspersky

Dati di rilevamento globali: utenti colpiti

In questa sezione vengono evidenziati i dati a livello globale e regionale osservati da Kaspersky nel 2021, che vengono confrontati con quelli degli anni precedenti.

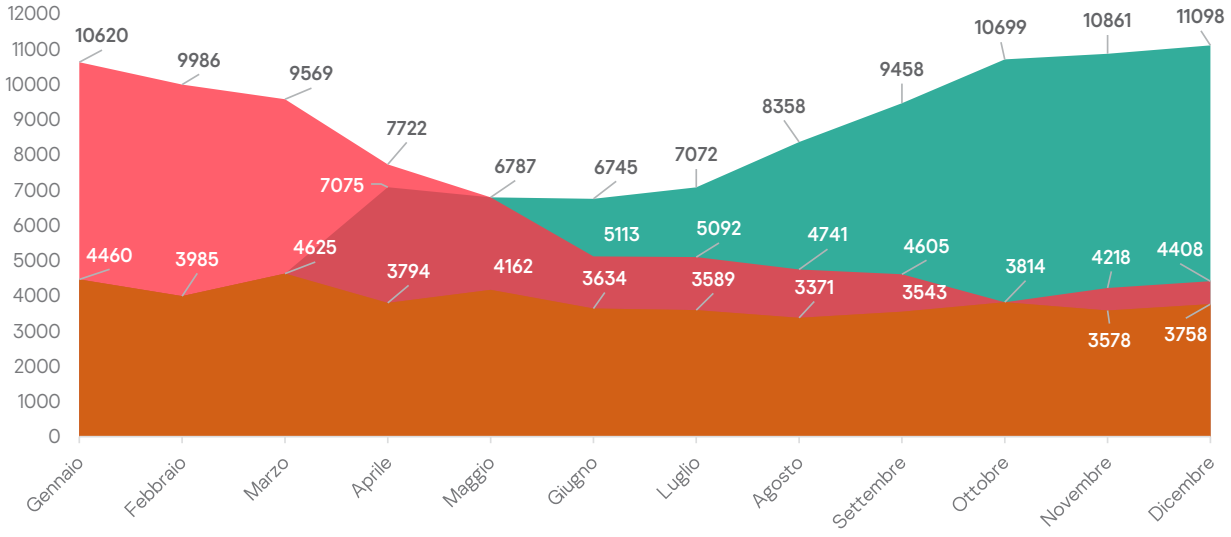
Nel 2021, lo stalkerware ha colpito un totale di 32.694 singoli utenti

Nel 2021, lo stalkerware ha colpito un totale di 32.694 singoli utenti. Il grafico seguente mostra l'evoluzione degli utenti colpiti su base annua a partire dal 2018.



L'evoluzione degli utenti colpiti su base annua a partire dal 2018

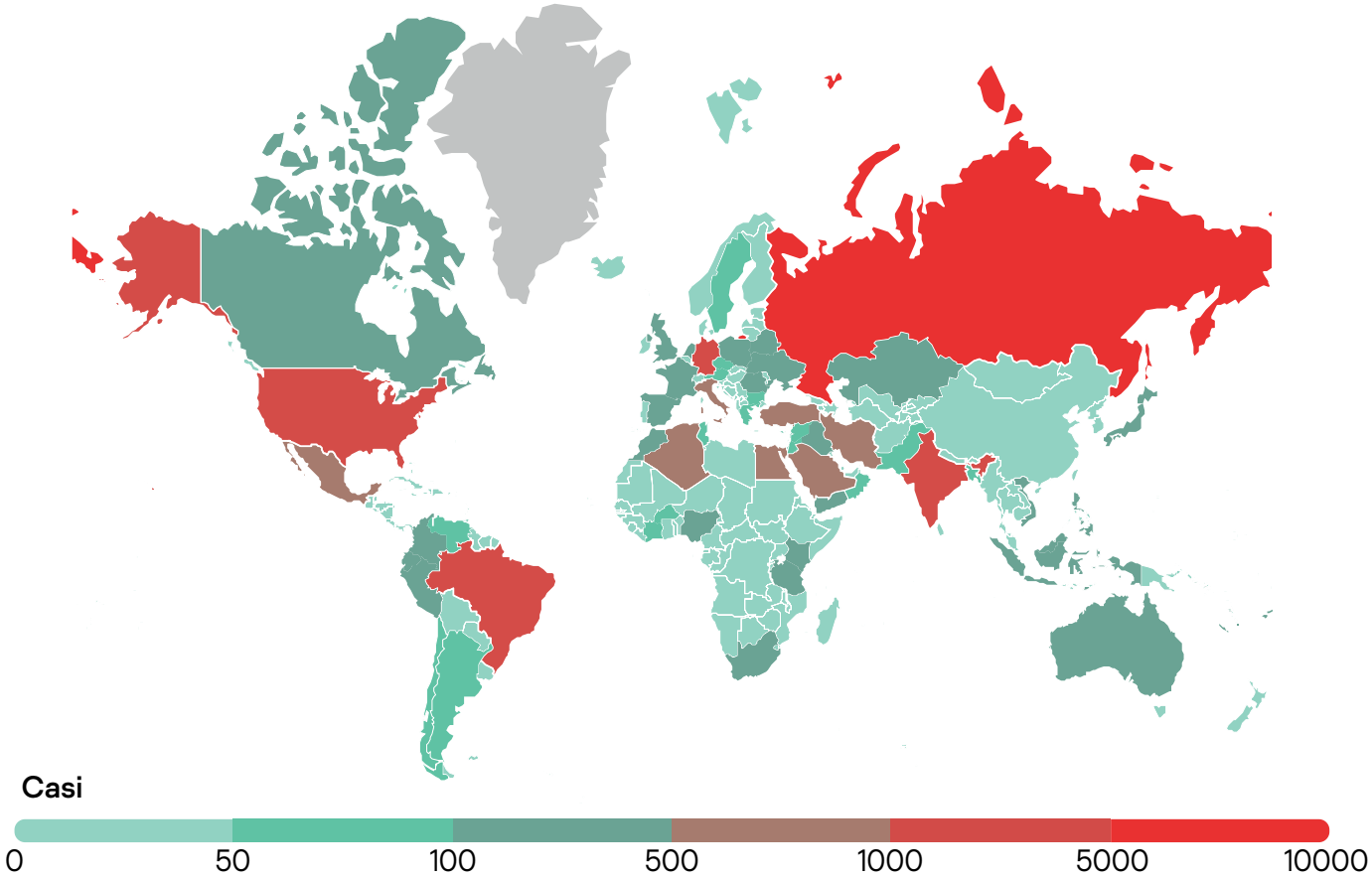
Il grafico sotto evidenzia gli utenti colpiti per mese nel periodo 2019-2021. Possiamo vedere come il trend nel 2021 sia risultato più stabile rispetto al 2020, in cui si osserva un vistoso calo nei mesi in cui vi è stato l'impatto del lockdown e delle misure di quarantena.



Utenti colpiti unici al mese nel period 2019-2021

Dati di rilevamento su base globale e regionale: geografica degli utenti colpiti

Lo stalkerware continua a colpire le persone nel mondo: nel 2021, Kaspersky ha rilevato utenti colpiti in 185 paesi o territori.



Metodologia

I dati di questo report sono ricavati dalle statistiche di minacce aggregate ottenute da Kaspersky Security Network, l'infrastruttura di Kaspersky dedicata all'elaborazione dei flussi di dati di cybersicurezza inviati da milioni di partecipanti volontari in tutto il mondo. Tutti i dati ricevuti vengono resi anonimi. Il calcolo delle statistiche si basa sull'analisi delle soluzioni di sicurezza per mobile di Kaspersky della linea consumer applicando solo i criteri di rilevamento stalkerware della Coalition Against Stalkerware. Ciò significa che gli utenti colpiti sono stati presi di mira solo dallo stalkerware. Non sono incluse nelle statistiche altre tipologie di app di monitoraggio o spyware che non rientrano nella definizione della Coalizione.

I dati statistici riguardano gli utenti mobile colpiti dallo stalkerware: ciò è diverso dal numero di rilevamenti. Il numero di rilevamenti può infatti essere più elevato in quanto può capitare di rilevare uno stalkerware per diverse volte sullo stesso dispositivo dello stesso utente, se quest'ultimo ha deciso di non rimuovere l'app dopo aver ricevuto la nostra notifica.

Infine, le statistiche tengono conto solo degli utenti mobile che utilizzano le soluzioni di sicurezza informatica di Kaspersky. Alcuni utenti potrebbero utilizzare un'altra soluzione di sicurezza informatica, altri non utilizzare nessuna soluzione.

Come nel 2020, Russia, Brasile, USA e India sono ancora una volta i primi quattro paesi in cui sono stati identificati il maggior numero di singoli utenti colpiti. È interessante notare che il Messico è sceso dal quinto al nono posto di questa classifica, mentre fanno il loro ingresso tra i top ten Algeria, Turchia e Egitto. Questi paesi prendono il posto di Italia, Regno Unito e Arabia Saudita, che non rientrano più tra i 10 primi paesi più colpiti dallo stalkerware.

	Paese	Utenti colpiti
1	Federazione Russa	7541
2	Brasile	4807
3	USA	2319
4	India	2105
5	Germania	1012
6	Iran	891
7	Algeria	665
8	Turchia	660
9	Messico	657
10	Egitto	640

Tabella 1 – I primi 10 paesi colpiti da stalkerware nel 2021 – su base globale

Nel rapporto di quest'anno forniamo dati statistici regionali più dettagliati riportando i numeri relativi a Europa, Asia-Pacifico, America Latina, Nordamerica, Europa orientale (esclusi i paesi dell'UE), Russia and Asia centrale, Medio Oriente e Africa.

In Europa, nel 2021 il numero complessivo di singoli utenti colpiti è stato di 4.236. Germania, Italia e Regno Unito sono in cima alla lista, mantenendo le stesse posizioni dello scorso anno. L'Austria è stata rimpiazzata nella top 10 dalla Repubblica Ceca.

	Paese	Utenti colpiti
1	Germania	1012
2	Italia	611
3	Regno Unito e Irlanda del Nord	430
4	Francia	410
5	Polonia	321
6	Spagna	321
7	Olanda	165
8	Romania	125
9	Belgio	94
10	Repubblica Ceca	82

Tabella 2 – I primi 10 paesi colpiti da stalkerware nel 2021 - Europa

In Europa orientale (esclusi i paesi dell'UE), Russia and Asia centrale, il numero totale di singoli utenti colpiti è di 9.207. I primi tre paesi colpiti sono Russia, Ucraina e Kazakistan.

	Paese	Utenti colpiti
1	Federazione Russa	7541
2	Ucraina	490
3	Kazakistan	461
4	Bielorussia	250
5	Uzbekistan	223
6	Azerbaigian	92
7	Repubblica Moldava	51
8	Tagikistan	49
9	Kirghizistan	40
10	Turkmenistan	19

Tabella 3 – I primi 10 paesi colpiti da stalkerware nel 2021 - Europa orientale (esclusi i paesi dell'UE), Russia and Asia centrale

In Medio Oriente e Africa, il numero totale di utenti colpiti nell'intera regione è di 6.270, con Turchia, Egitto e Arabia Saudita ad avere il maggior numero di utenti interessati.

	Paese	Utenti colpiti
1	Turchia	660
2	Egitto	640
3	Arabia Saudita	575
4	Kenya	271
5	Sudafrica	240
6	Emirati Arabi Uniti	143
7	Nigeria	123
8	Kuwait	68
9	Oman	58
10	Etiopia	46

Tabella 4 – I primi 10 paesi colpiti da stalkerware nel 2021 – Medio Oriente e Africa

Nella regione Asia-Pacifico il numero totale di utenti colpiti è di 4.243. India è sostanzialmente avanti rispetto ad altri paesi, con 2.105 singoli utenti colpiti. È seguita da Indonesia e Vietnam.

	Paese	Utenti colpiti
1	India	2105
2	Indonesia	353
3	Vietnam	258
4	Filippine	240
5	Malesia	229
6	Australia	205
7	Bangladesh	169
8	Giappone	167
9	Pakistan	98
10	Sri Lanka	83

Tabella 5 - I primi 10 paesi colpiti da stalkerware nel 2021 - Asia Pacifico

La classifica di America Latina e Caraibi è dominata da un paese, il Brasile, che rappresenta il 72,5% del numero totale di utenti colpiti nella regione (e rappresenta anche il 32% circa della popolazione della regione). Il Brasile è seguito da Messico e Colombia. L'intera regione presentava 6.609 utenti colpiti.

	Paese	Utenti colpiti
1	Brasile	4807
2	Messico	657
3	Colombia	202
4	Ecuador	192
5	Perù	179
6	Argentina	90
7	Cile	73
8	Venezuela	58
9	Bolivia	46
10	Haiti	36

Tabella 6 – I primi 10 paesi colpiti da stalkerware nel 2021 – America Latina

Per finire, nel Nordamerica gli USA rappresentano l'87% di tutti gli utenti colpiti della regione, un dato atteso, dal momento che gli USA hanno una popolazione di dieci volte quella del Canada. Il numero totale di utenti colpiti nel Nordamerica, escluso il Messico che viene incluso nell'America Latina, è di 2.666.

	Paese	Utenti colpiti
1	USA	2319
2	Canada	347

Tabella 7 – Utenti del 2021 colpiti da stalkerware – Nord America

Funzionalità comuni delle applicazioni stalkerware

In questa sezione sono elencate le applicazioni stalkerware più utilizzate per controllare i dispositivi mobili a livello globale. Cerberus e Reptilicus risultano essere le applicazioni stalkerware più usate, rispettivamente con 5.575 e 4.417 utenti colpiti a livello globale.

	Nome applicazione	Utenti colpiti
1	Cerberus	5,575
2	Reptilicus (anche noto come Vkurse)	4,417
3	Track My Phones	1,919
4	AndroidLost	1,731
5	MobileTracker Free	1670
6	Hoverwatch	1,094
7	wSpy	1,050

Tabella 8 – Classifica delle principali applicazioni stalkerware nel 2021

Le applicazioni stalkerware possono offrire un enorme potere e facile accesso ai loro utilizzatori, a seconda delle applicazioni e se vengono utilizzate in modalità gratuita o a pagamento. Alcune di esse vengono commercializzate come applicazioni antifurto o di parental control, ma si differenziano da queste in diversi modi, a partire dal fatto che operano in modalità stealth, dunque senza il consenso della vittima.

Gran parte delle applicazioni più diffuse contengono comuni funzionalità stalkerware come ad esempio:

- Icona nascondi app
- Lettura di SMS, MMS e registro chiamate
- Acquisizione lista contatti

I sistemi Android OS e iOS sono ugualmente colpiti da stalkerware?

Gli stalkerware sono meno frequenti sugli iPhone rispetto ai dispositivi Android poiché iOS è tradizionalmente un sistema chiuso. Tuttavia il perpetratore può aggirare questo limite agendo sugli iPhone sbloccati tramite jailbreaking, ma deve sempre avere accesso fisico al telefono per eseguire il jailbreaking. Gli utenti iPhone che temono di essere sorvegliati dovrebbero sempre tener d'occhio il proprio dispositivo.

In alternativa, l'abusante può offrire alla sua vittima un iPhone, o qualsiasi altro dispositivo, con lo stalkerware preinstallato. Sono molte le società che offrono questi servizi online, permettendo al persecutore di far installare questi tool su un telefono nuovo, che poi può essere consegnato in confezione regalo alla futura vittima.

- Localizzazione GPS
- Ricerca eventi in calendario
- Lettura di messaggi dai servizi di messaggistica e social network più popolari, come Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr, Weico, Reddit ecc.
- Visualizzazione di foto e immagini dalle gallerie immagini dei cellulari
- Riprendere screenshot
- Fare selfie

L'uso dello stalkerware sembra diminuire, ma non la violenza

Il numero di utenti colpiti e alcuni dei comportamenti e percezioni intorno all'uso dello stalkerware destano sempre preoccupazioni

Se è vero che i nostri dati sul 2020 evidenziano un calo del 39% di utenti colpiti, la lotta contro lo stalkerware e la cyber-violenza è lungi dall'essere terminata. Il numero di utenti colpiti e alcuni dei comportamenti e percezioni intorno all'uso dello stalkerware destano sempre preoccupazioni. Nel novembre 2021, Kaspersky ha commissionato una ricerca globale su oltre 21.000 partecipanti di 21 paesi, esaminando il loro atteggiamento nei confronti della privacy e dello stalking digitale nell'ambito dei rapporti intimi. Se da un lato la maggioranza degli intervistati (il 70%) non ritiene una cosa accettabile controllare il proprio partner senza il suo consenso, una percentuale significativa di soggetti (il 30%) non vede nessun problema in questo e lo trova accettabile in talune circostanze. Di coloro che pensano che ci siano ragioni giustificabili per mettere in atto una sorveglianza segreta, quasi due terzi adotterebbero questo comportamento se avessero ragione di credere che il proprio partner è infedele (il 64%) o se riguardasse la loro sicurezza (63%), mentre la metà dei soggetti attuerebbe il controllo se credesse che il proprio partner è coinvolto in attività criminose (50%).

Le tecnologie dell'informazione e della comunicazione sono potenti strumenti a disposizione dei persecutori per esercitare un controllo coercitivo, specialmente in quelle relazioni in cui è già presente la violenza offline

La disponibilità di Internet ad alta velocità, unitamente alla rapida diffusione della tecnologia dell'informazione e della comunicazione (ICT), ha dato impulso alla cyber-violenza, offrendo ai persecutori un ulteriore strumento per condividere contenuti violenti o pericolosi o per attuare comportamenti che creano danno emotivo, psicologico o fisico. Se da un lato queste tecnologie hanno offerto alle persone la possibilità di mantenere relazioni sociali ed emotive anche a grande distanza, la tecnologia ICT ha però anche alimentato la cyber-violenza, una conseguenza i cui vasti effetti si estendono al mondo offline con reali impatti negativi sulle sue vittime.

I risultati della nostra indagine avvalorano quanto detto: il 15% degli intervistati di tutto il mondo sostiene di avere installato un'app di monitoraggio su richiesta del proprio partner, mentre il 34% di questi dice di avere sperimentato abusi fisici e/o verbali dal proprio partner intimo.

Se è prematuro giungere a una conclusione definitiva riguardo al calo di utenti colpiti nel 2021, vi sono due teorie che potrebbero spiegare questo trend.

Per prima cosa, riteniamo che ogni aspetto della nostra vita risenta tuttora pesantemente della pandemia. Recenti studi dimostrano che stanno emergendo nuovi comportamenti in settori della vita come lavoro, istruzione, casa, consumi, comunicazioni e informazione, viaggi e mobilità. Per dirla in breve, le persone stanno di più a casa (il 49% evita di uscire di casa mentre il 50% lavora da casa part-time o per l'intera giornata), hanno ridotto le interazioni personali (il 57% sostiene di essersi socialmente distanziato dagli amici e dalla comunità) e gli spostamenti, mentre crescono shopping, didattica e intrattenimento online. Dal punto di vista di un abusante, ciò può comportare il venire meno della necessità di spiare il proprio partner, in quanto è a lui presente per la maggior parte del tempo.

Secondo, oggi Internet of Things (IoT) e la digitalizzazione hanno pervaso le nostre vite. Riempiono le nostre routine quotidiane e le nostre abitazioni, auto e uffici. Se da un lato ciò comporta infinite opportunità e vantaggi, dall'altro molti dispositivi consentono anche il tracking da terze parti. La nostra ricerca suggerisce che il persecutore potrebbe anche utilizzare altri mezzi, oltre allo stalkerware, per tracciare il proprio partner; il 50% dei partecipanti al nostro sondaggio sostiene di essere stato tracciato attraverso le app del telefono, un altro 29% sostiene di essere stato tracciato attraverso i dispositivi di tracciatura, il 22% attraverso webcam e il 18% tramite i dispositivi smart home.

La recente pubblicazione nel gennaio 2020 da parte di Apple di un manuale di sicurezza per il suo prodotto AirTag segna un cambiamento di direzione nella percezione della situazione.

NNEDV, la National Network to End Domestic Violence (Rete nazionale per la fine della violenza domestica) e WWP EN, la European Network for the Work with Perpetrators of Domestic Violence, network europeo che lavora con soggetti autori di violenza domestica, condividono con noi la loro esperienza e le loro opinioni riguardo a queste due teorie e in generale sull'abuso compiuto con l'ausilio della tecnologia.

In che modo le misure imposte dai governi nel periodo pandemico hanno facilitato e rafforzato il controllo coercitivo dei persecutori —

Berta Vall Castelló, Responsabile ricerca e sviluppo e Anna McKenzie, Responsabile comunicazioni WWP EN

Per controllo coercitivo si intende "un modello di comportamento abusivo pensato per esercitare il dominio e il controllo sull'altro soggetto in una relazione intima. Può includere una serie di comportamenti abusivi (fisici, psicologici, emotivi o finanziari), il cui effetto cumulative nel tempo priva le vittime-sopravvissuti della loro autonomia e indipendenza come individui" (McGorrery and McMahon, 2020). Come scriviamo nel nostro manuale "Same Violence, New Tools – How to work with violent men who use cyberviolence," (Stessa violenza, nuovi strumenti. Come lavorare con gli uomini violenti che usano la cyber-violenza), i persecutori isolano i loro partner e li rendono emotivamente dipendenti. Ricorrono ad aggressioni, minacce, intimidazioni, umiliazioni, isolamento e altro ancora al fine di creare una sensazione costante di paura, nonché in generale un venir meno del senso di libertà. Le tecnologie dell'informazione e della comunicazione sono potenti strumenti a disposizione dei persecutori per esercitare un controllo coercitivo, specialmente in quelle relazioni in cui è già presente la violenza offline.

Un recente studio sulla violenza domestica durante la pandemia da COVID-19 ha dimostrato che le misure imposte dai governi durante il lockdown hanno di fatto facilitato e rafforzato il controllo coercitivo dei persecutori. Gli autori dello studio suggeriscono che le condizioni di isolamento/distanziamento fisico imposte dai governi si sono sommate alle strategie di controllo coercitivo utilizzate dai persecutori per controllare i loro partner (Pentaraki and Speake, 2020). Sulla base di questi risultati, appare probabile come i persecutori sentano meno la "necessità" di ricorrere allo stalkerware per esercitare un controllo coercitivo sui loro partner. Inoltre, come osserva una recente ricerca, gli abusi compiuti con l'ausilio della tecnologia spesso tendono a crescere durante un periodo di separazione (George and Harris 2014; Woodlock 2016). Pertanto, in una situazione di lockdown in cui le coppie sono state costrette a stare in casa insieme, i persecutori erano meno inclini a compiere abusi con l'ausilio della tecnologia.

WWP EN

La European Network for the Work With Perpetrators of domestic violence (WWP EN) è un'associazione di organizzazioni che direttamente o indirettamente lavorano con persone che commettono violenza nell'ambito di rapporti intimi. La rete WWP EN si focalizza sugli atti di violenza perpetrati dagli uomini contro donne e bambini. La missione di WWP EN è migliorare la sicurezza delle donne e dei loro bambini e di altri soggetti a rischio di violenza nei rapporti intimi, promuovendo un'opera efficace con coloro che commettono questo tipo di violenza, perlopiù uomini.

www.work-with-perpetrators.eu/experiencing-violence

Le misure imposte dai governi durante il lockdown hanno di fatto facilitato e rafforzato il controllo coercitivo dei persecutori

Occorre ricordare che un minore uso dello stalkerware non equivale a un calo della violenza del partner intimo (IPV) durante la pandemia. Al contrario, Boxall, Morgan e Brown (2020) osservano che la violenza è cresciuta durante la pandemia da COVID-19. Pertanto i risultati di questo report indicano che lo stalkerware è stato sostituito da altri strumenti. Come sottolinea Elena Gajotto della ONG italiana Una Casa per l'Uomo: "Oggi è talmente facile monitorare e tracciare qualcuno, ad esempio usando il suo account Google, che non serve nemmeno ricorrere allo stalkerware". Nello specifico, stante l'ampia varietà di abusi facilitati dalla tecnologia, vi può essere stato un impatto sull'uso dello stalkerware. Letizia Baroncelli, della ONG italiana Centro Ascolto Uomini Maltrattanti (CAM), concorda e aggiunge: "Penso che vediamo meno stalkerware solo perché ci sono tanti altri modi di perpetrare abusi online".

Tuttavia, ONG, governi e ricercatori segnalano dall'inizio della pandemia una sostanziale crescita di abusi basati sull'immagine e fenomeni di sextortion (Boniello, 2020; CCRI, comunicazione personale, 2 giugno 2020; FBI, 2020, 2021). Sembra che vi sia un'escalation di questo tipo di abuso facilitato dalla tecnologia, soprattutto tra i teenager e le coppie che non vivono sotto lo stesso tetto. Come osserva Letizia Baroncelli: "La condivisione di foto personali si è molto diffusa dall'inizio della pandemia, soprattutto tra i persecutori giovani, che non capiscono che stanno commettendo un reato". Aggiunge Elena Gajotto: "Gli abusi basati su immagini provocano un danno devastante alle donne colpite, mentre gli uomini non si rendono nemmeno conto di aver fatto qualcosa di male".

Diversi membri di WWP EN concordano sul fatto che la forma più comune di violenza digitale è quella dell'uomo che controlla le attività digitali del proprio partner, ad esempio e-mail, telefonate e account sui social. Questo è in linea con le osservazioni di Daniel Antunovic della ONG croata UZOR, che concorda sul fatto che le forme 'primitive' di stalking digitale sono quelle in cui d'imbatte più sovente.

Alla WWP EN, riteniamo sia fondamentale focalizzarci sugli abusi facilitati dalla tecnologia per garantire la sicurezza delle vittime. Aggiunge Elena Gajotto: "La metà circa degli uomini condivide la violenza digitale esercitata, senza rendersi conto che questo è un abuso. Se nel nostro lavoro con i persecutori non ci focalizziamo esplicitamente su questo tipo di violenza, questo aspetto non viene fuori". Vi è quindi la necessità di potenziare la capacità dei

professionisti che lavorano con i persecutori e dei professionisti che lavorano con le vittime di violenza domestica di eseguire screening e intervenire nei casi di violenza domestica. Come osserva Daniel Antunovic: "Non abbiamo riscontrato il numero di casi di violenza digitale che ci aspettavamo dall'inizio della pandemia. Tuttavia l'abuso facilitato dalla tecnologia è in qualche modo assimilabile alla violenza sessuale. Accade di frequente, ma rimane nascosto".

NNEDV

Il Progetto NNEDVs Safety Net si focalizza sull'incrocio di tecnologia, privacy, riservatezza e innovazione, in quanto si collega ai temi di sicurezza e degli abusi sostenendo politiche, educando e formando sostenitori e professionisti nel sistema giudiziario, e lavorando con comunità, enti e società di tecnologia per contrastare gli abusi compiuti con la tecnologia, supportare i sopravvissuti nell'uso della tecnologia, e sfruttare la tecnologia per migliorare i servizi.

https://nnedv.org/content/mission-vision/

Sempre più "dispositivi smart" vengono utilizzati nei casi di violenza del partner intimo — Toby Shulruff, Project manager sicurezza tecnologica presso la NNEDV

Se è vero che lo stalkerware è un problema comune, vi sono molti altri strumenti a disposizione per compiere abusi che possono apparire stalkerware, ma non lo sono. Ad esempio, i dati personali disponibili online e le funzionalità quotidiane di dispositivi e account possono essere utilizzati per localizzare una persona o tracciare le sue attività. La complessità e i collegamenti tra dispositivi, account e informazioni su Internet possono rendere difficile alle vittime e a chi lavora con loro valutare ciò che sta succedendo, ed implementare una risposta efficace. Per un sopravvissuto può essere terribile e devastante realizzare che un abusante conosce molti dettagli della sua vita quotidiana.

Purtroppo, cresce anche il numero di dispositivi smart, tra cui home assistant, elettrodomestici connessi e sistemi di sicurezza collegati alle reti WiFi e agli smartphone, che vengono utilizzati in casi di violenza del partner intimo.

In uno studio condotto da NNEDV nel dicembre 2020 e gennaio 2021, le risposte raccolte hanno rivelato un incremento di ogni tipologia di abuso con tecnologia durante la pandemia. Se i telefoni rappresentano la tecnologia più spesso abusata, la valutazione delle necessità di NNEDV evidenzia che questo è il caso nell'87% delle volte; anche i dispositivi smart o connessi sono stati individuati come tecnologie sempre più utilizzate nel contesto di abusi compiuti con la tecnologia, come regolarmente constatato da un terzo circa dei professionisti di supporto.

Cresce anche il numero di dispositivi smart, tra cui home assistant, elettrodomestici connessi e sistemi di sicurezza collegati alle reti WiFi e agli smartphone, che vengono utilizzati in casi di violenza del partner intimo

È probabile che questo trend cresca, di pari passo con il crescere del numero di soggetti che utilizzano dispositivi IoT. Questi prodotti sono progettati per migliorare comodità ed efficienza. La produzione di dispositivi IoT costituisce un mercato globale in rapida crescita, in cui operano player più grandi consolidati a fianco di molte nuove società[1] di minori dimensioni. Internet of things è resa possibile da una sovrapposizione di diverse tendenze di tecnologia: miniaturizzazione, maggiore capacità di elaborazione, maggiore spazio di archiviazione dati, minori costi di produzione e connettività.

Per effetto di una varietà di fattori (pressioni del mercato, rapido emergere della tecnologia e complessità di IoT), sono sempre più evidenti[2] gravi rischi per la sicurezza e la privacy. I dispositivi smart home in particolare vengono utilizzati in un contesto di violenza del partner intimo per controllare, minacciare e causare danno alla vittima. [Ricercatori impegnati nel Progetto Gender + IoT presso la University College London[3] studiano questi danni] [e propongono rimedi in partnership con i professionisti del supporto nel campo].

La recente valutazione delle esigenze di NNEDV ha documentato una crescita delle tattiche di abuso compiuto con la tecnologia durante la pandemia. Il nostro timore è che mentre usciamo da questa crisi sanitaria pubblica, i persecutori che hanno adottato queste tattiche o hanno incrementato l'abuso della tecnologia in questo periodo non saranno incentivati a smettere di utilizzare questa forma d'abuso. Una recente ricerca[4] suggerisce che i professionisti del supporto dovrebbero chiedere informazioni su tutte le tipologie di abusi compiuti con la tecnologia, inclusi stalkerware e dispositivi smart home. È molto probabile che il picco di abusi compiuti con la tecnologia documentato dai professionisti del supporto non sia destinato a scomparire. È essenziale continuare a supportare le vittime, e lavorare per prevenire gli abusi compiuti con la tecnologia.

1 Internet Society. (2015). The Internet of Things: An overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

2 Internet Society. (2015). The Internet of Things: An overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

3 Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). The rise of the Internet of Things and implications for technology-facilitated abuse. University College London.

4 Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. Proceedings of the ACM on human-computer interaction, 1(CSCW), p.1-22.

In che modo Kaspersky e i suoi partner stanno collaborando per combattere lo stalkerware

La minaccia dello stalkerware non è soltanto un problema tecnico: vanno coinvolte tutte le parti della società nel risolvere il problema. In questi ultimi anni Kaspersky è in prima linea nel trattare il problema dello stalkerware. Stiamo contattando stakeholder pubblici e privati per meglio comprendere il problema e trovare soluzioni comuni. Stiamo contribuendo allo sviluppo di materiale per la formazione e strumenti per supportare organizzazioni no-profit, società, istituzioni e individui nello sviluppo della resilienza allo stalkerware. Stiamo organizzando e prendiamo parte a webinar e tavole rotonde con le istituzioni per condividere le nostre opinioni e contribuire ai dibattiti che plasmeranno la legislazione del domani.

Kaspersky è uno dei cofondatori e promotori della Coalition Against Stalkerware (CAS), un gruppo di lavoro internazionale impegnato ad affrontare lo stalkerware e a combattere la violenza domestica. La Coalizione raggruppa organizzazioni che lavorano a fianco di vittime e abusanti, attivisti digitali e fornitori di soluzioni di cybersicurezza. È una piattaforma unica che permette a tutti gli stakeholders coinvolti di condividere le best practice e unire le forze per affrontare il problema dello stalkerware.

Kaspersky figura inoltre tra i partner del progetto DeStalk. Finanziato dalla Commissione Europea, questo progetto di ricercar mira a sviluppare una strategia per formare e supportare i professionisti che operano nell'ambito dei servizi di supporto alle vittime e che lavorano ai programmi di recupero dei persecutori, funzionari di istituzioni ed enti locali, insieme ad altri gruppi attinenti. Il consorzio intende ammodernare e testare gli strumenti esistenti per gli operatori e sta sviluppando una campagna di sensibilizzazione pilota regionale in Italia.

Nel 2021 abbiamo fatto squadra con l'INTERPOL e due organizzazioni no-profit consolidate negli USA e in Australia per offrire ai funzionari di polizia due sessioni di formazione online. A questi corsi hanno preso parte 210 partecipanti da tutto il mondo.

Alla fine del 2021, Kaspersky ha inoltre preso parte a "Combating violence against women in a digital age - utilising the Istanbul Convention" (Combattere la violenza sulle donne nell'era digitale utilizzando la convenzione di Istanbul), un evento organizzato dal Consiglio d'Europa. Tale evento ha offerto l'opportunità di discutere le raccomandazioni del Gruppo di esperti sulla lotta alla violenza nei confronti delle donne e la violenza domestica (GREVIO).

TinyCheck: uno strumento a supporto delle vittime di violenza domestica

Merita ricordare l'iniziativa di Kaspersky con il tool TinyCheck. Si tratta di uno strumento open-source gratuito sviluppato e supportato da Kaspersky. Inizialmente creato per aiutare le organizzazioni no profit a proteggere le vittime di violenza domestica e tutelare la loro privacy, TinyCheck facilita il rilevamento di stalkerware sui dispositivi della vittima e su qualsiasi sistema operativo in modo semplice, veloce e non invasivo, senza che il persecutore se ne accorga. Mentre le soluzioni di sicurezza possono monitorare e notificare l'utente sulla presenza di stalkerware, esse vanno però installate sul dispositivo, e dunque vi è il rischio che anche il persecutore venga allertato. Soluzioni come il tool TinyCheck fanno invece in modo che il sopravvissuto possa utilizzare il suo dispositivo senza timore di essere sorvegliato.

TinyCheck facilita il rilevamento di stalkerware sui dispositivi della vittima e su qualsiasi sistema operativo in modo semplice, veloce e non invasivo, senza che il persecutore se ne accorga

Con TinyCheck, non è necessario installare nessuna applicazione sul dispositivo per eseguire il controllo, mentre i risultati dell'ispezione non vengono visualizzati né trasmessi al dispositivo potenzialmente infettato. Inoltre TinyCheck permette alla vittima di monitorare qualsiasi dispositivo, sia che utilizzi iOS, Android o altro sistema operativo. Queste funzioni affrontano i due problemi principali nella lotta per proteggere gli utenti contro lo stalkerware. Questo tool è stato sviluppato per girare su un Raspberry Pi, utilizzando una regolare connessione Wi-Fi. TinyCheck analizza rapidamente il traffico in uscita di un dispositivo mobile e individua gli indicatori di compromissione (IOCs), ad esempio le interazioni con fonti di malware conosciute, come i server legati allo stalkerware. Allo stato attuale il tool utilizza IOC raccolti non solo dai ricercatori Kaspersky, ma anche provenienti dagli archivi gestiti da ricercatori di soluzioni di security indipendenti (un ringraziamento speciale va a Etienne Maynier, noto anche come Tek, di Echap e a Cian Heasley). Auspichiamo che la comunità prosegui questo lavoro, tenendo gli IOC aggiornati.

Ciò detto, vanno compresi i limiti di TinyCheck. Questo tool va utilizzato tenendo ben presente questa avvertenza: gli IOC non offrono un rilevamento completo in tempo reale di tutte le app stalkerware come fa una Soluzione di sicurezza IT. Pertanto, in presenza di un risultato che non rileva nessun stalkerware non si può escludere la possibilità che lo stalkerware sia stato installato ma non rilevato da TinyCheck.

Nel corso del 2021, altre organizzazioni no profit nel campo della violenza domestica hanno testato TinyCheck e hanno fornito il loro feedback per aiutare a migliorare il servizio. Anche le forze di polizia e gli organi giudiziari di vari paesi hanno espresso il loro interesse per questo strumento a supporto delle vittime di violenza.

Il 2021 ha visto sviluppi positivi sui fronti della regolamentazione e istituzionale

In tutto il mondo il 2021 ha visto alcuni sviluppi positivi nella lotta contro lo stalkerware dal punto di vista della regolamentazione e istituzionale. Nel maggio 2021 la Dieta, il parlamento giapponese, ha approvato un disegno di legge che intende emendare la normativa sugli stalker. In base alla legge riformata, in aggiunta ad altre clausole, è ora illegale ottenere informazioni sulla localizzazione degli smartphone delle persone tramite app senza la loro autorizzazione.

Nell'agosto 2021, la Federal Trade Commission negli USA ha vietato a un creatore di app di commercializzare stalkerware. Si tratta della prima messa al bando questo tipo.

Il 17 agosto 2021 il parlamento tedesco ha approvato un "Disegno di legge per emendare il codice penale – Combattere più efficacemente lo stalking e migliore copertura del cyberstalking". La nuova legge, entrata in vigore il 1° ottobre 2021, ora include il cyberstalking nel catalogo dei reati. Questo cambiamento avviene sulla spinta del costante progresso tecnologico e della conseguente crescita del cyberstalking, in particolare attraverso le app di stalking o lo stalkerware. Inoltre vi è una sezione importante della nuova legge che classifica un caso come grave se il trasgressore "nel corso di reato, utilizza un programma informatico allo scopo di attuare lo spionaggio digitale di altre persone".

Il Consiglio d'Europa è stato molto attivo su questo tema nel corso del 2021. Nella sua prima raccomandazione sulla "dimensione digitale" della violenza contro le donne, il Gruppo di esperti/e sulla lotta contro la violenza nei confronti delle donne e la violenza domestica (GREVIO) del Consiglio d'Europa definisce e descrive i problemi della violenza di genere commessi online e degli attacchi compiuti con la tecnologia contro le donne, come i dispositivi di tracciamento legalmente acquistabili che consentono ai persecutori di attuare stalking contro le loro vittime. A questa iniziativa ha fatto seguito nel dicembre 2021 una relazione d'iniziativa legislativa sulla cyber-violenza di genere che è stata approvata dal Parlamento Europeo. Il rapporto chiede (i) una definizione comune della cyber-violenza di genere e (ii) lo sviluppo delle capacità per gli stakeholder. Colloca lo stalkerware tra i principali metodi di cyber-violenza e "respinge la nozione che le applicazioni stalkerware si possano considerare applicazioni di parental control". Seguendo le raccomandazioni generali del Consiglio d'Europa, questo rapporto, seppur non vincolante, è un altro documento ufficiale che affronta il

problema dello stalkerware ed esorta gli stati membri a modificare le loro leggi e azioni per contrastare il problema. Per finire, l'8 marzo 2022 il Consiglio d'Europa ha pubblicato una proposta per una Direttiva del Parlamento Europeo e del Consiglio sulla lotta alla violenza nei confronti delle donne e la violenza domestica. Il documento prende in esame la cyber-violenza e dedica due articoli al cyber-stalking (Art 8) e alle cyber molestie (Art 9) che propone di criminalizzare.

Pensi di essere vittima di stalkerware? Ecco qualche suggerimento

Che siate o meno una vittima di stalkerware, ecco alcuni suggerimenti per proteggervi meglio:

Se hai bisogno di aiuto, rivolgiti a un'organizzazione di supporto locale. Per trovarne una vicino a te, visita il sito Web della Coalition Against Stalkerware

- Proteggete il vostro telefono con una password forte che non dovete condividere con il vostro partner, amici o colleghi
- Cambiate regolarmente le password di tutti i vostri account e non condividetele con nessuno
- Scaricate le app solo da fonti ufficiali, come Google Play o Apple App Store
- Installate sui dispositivi un sistema di sicurezza IT affidabile come Kaspersky Internet Security per Android ed eseguite regolarmente la scansione. Tuttavia, in caso di stalkerware potenzialmente già installato, questo andrebbe fatto solo dopo aver valutato il rischio per la vittima, dal momento che l'abusante potrebbe accorgersi che si sta utilizzando una soluzione per la cybersicurezza.

Le vittime di stalkerware possono essere vittime di un ciclo di abusi di maggiore portata, inclusi abusi fisici. In alcuni casi, il persecutore riceve un avviso se la sua vittima esegue una scansione del dispositivo o rimuove un'app stalkerware. In questo caso, ciò può comportare un aggravamento della situazione e ulteriori aggressioni. Ecco perché è importante procedere con cautela se pensate di essere vittima di stalkerware.

- **Rivolgetevi a un'organizzazione di supporto locale:** per trovarne una vicina a voi, visitate il sito Coalition Against Stalkerware.
- **Fate attenzione ai seguenti segnali di avvertimento:** questi possono essere il rapido esaurimento della batteria causato da app sconosciute o sospette che consumano la batteria e applicazioni installate di recente con accesso sospetto che utilizzano e tracciano la vostra posizione, inviano o ricevono messaggi di testo e interferiscono con altre attività personali. Verificate inoltre se l'opzione "sorgenti sconosciute" è attivata, potrebbe essere un segnale che un software indesiderato è stato installato da una fonte di terze parti. È importante sottolineare che questi segnali sono solo sintomi di una possibile installazione di stalkerware, non un'indicazione definitiva.
- **Non cercate di cancellare lo stalkerware, di cambiare qualsiasi impostazione o manomettere il vostro telefono:** questo potrebbe mettere in guardia il vostro potenziale persecutore e portare a un aggravamento della situazione. Inoltre rischiate di cancellare importanti dati o prove che potrebbero essere usati in un procedimento giudiziario.

Per ulteriori informazioni sulle nostre attività che riguardano gli stalkerware o qualsiasi altra richiesta, si prega di scrivere a ExtR@kaspersky.com.

La Coalition Against Stalkerware (coalizione contro gli stalkerware) è stata fondata a novembre del 2019 in risposta alla crescente minaccia rappresentata da questo fenomeno. La coalizione combina l'esperienza dei suoi partner nel sostegno alle vittime di violenza domestica, nel lavoro con i perpetratori e nel patrocinio dei diritti digitali per affrontare il comportamento criminale rappresentato dallo stalkerware. Tutti i membri si impegnano a combattere la violenza domestica, lo stalking e le molestie che sfruttano gli stalkwerware, sensibilizzando il pubblico su questo problema.

La Coalition Against Stalkerware (coalizione contro lo stalkerware):
https://stopstalkerware.org/

COALITION AGAINST STALKERWARE

Notizie sulle minacce informatiche: www.securelist.com
Notizie sulla sicurezza IT: business.kaspersky.com
Sicurezza informatica per piccole e medie imprese: www.kaspersky.it/small-to-medium-business-security
Sicurezza informatica per aziende Enterprise: www.kaspersky.it/enterprise-security

www.kaspersky.it

kaspersky