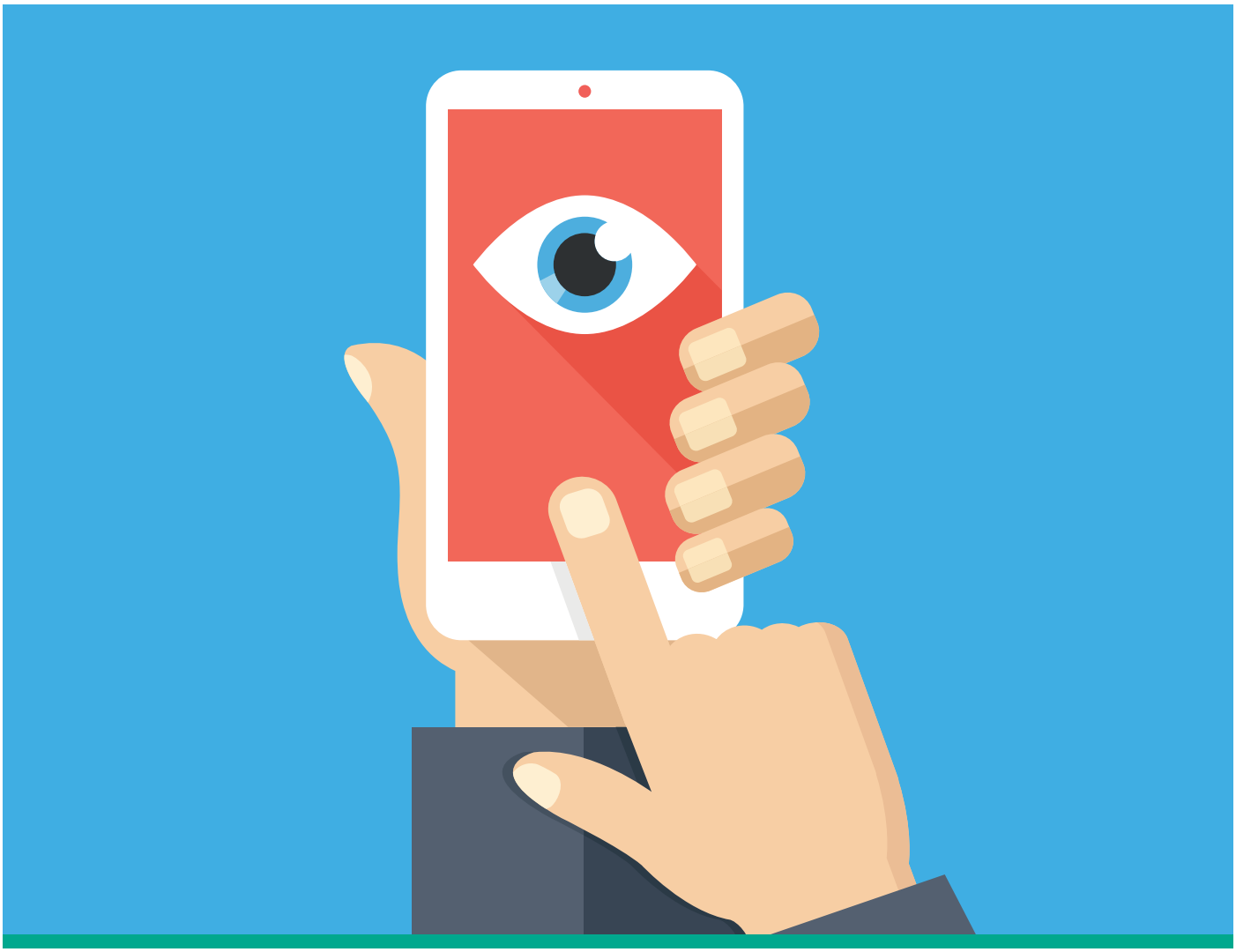


La situazione dello **stalkerware** nel 2020

COALITION AGAINST STALKERWARE

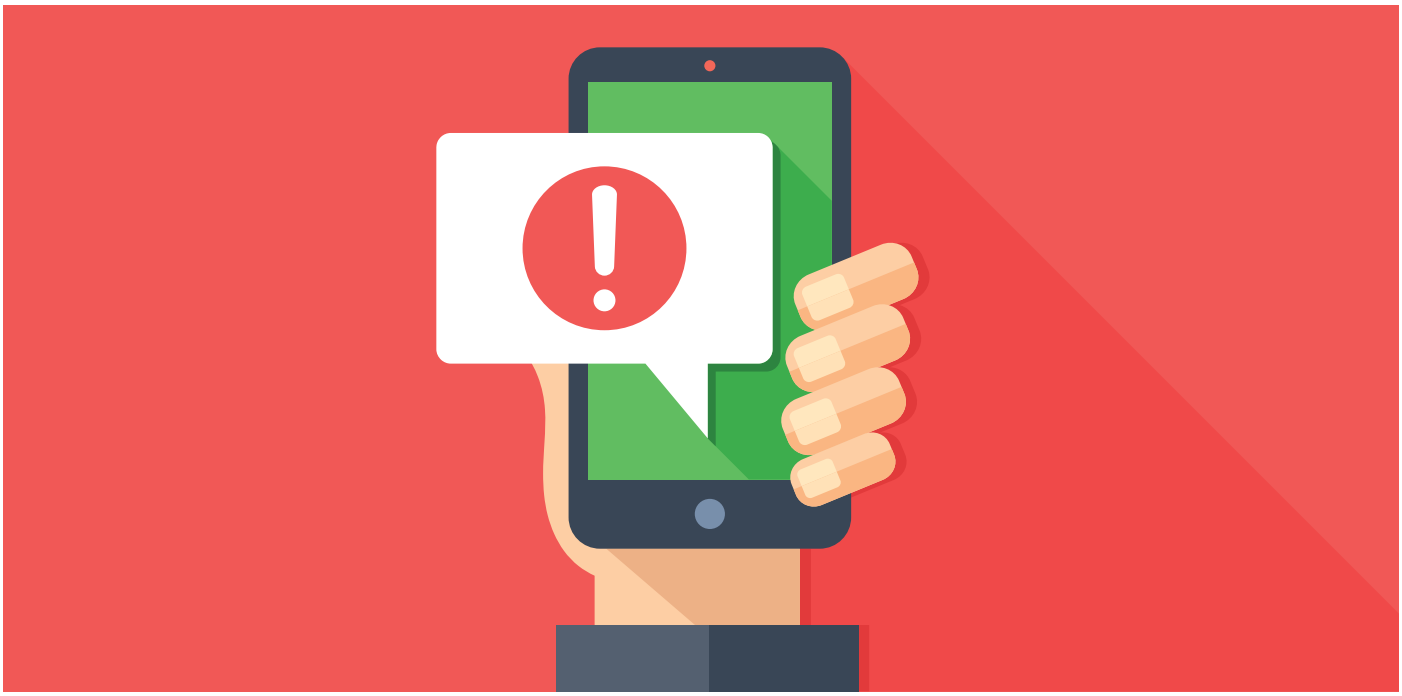
kaspersky

Indice

Principali osservazioni 2020

I dati di Kaspersky dimostrano che la portata del problema dello stalkerware nel 2020 non è migliorata di molto rispetto all'anno precedente:

- Il numero di persone colpite resta alto. Nel 2020 erano 53.870 i nostri utenti con dispositivi mobili colpiti da stalkerware a livello mondiale. Questi numeri includono solo gli utenti Kaspersky, di conseguenza i numeri complessivi risultano superiori. Alcuni degli utenti interessati da tale fenomeno utilizzano altre soluzioni di sicurezza informatica sui loro dispositivi, ma c'è chi non mette in atto alcuna soluzione.
- Con oltre 8.100 utenti colpiti a livello globale, Nidb risulta essere il sample di stalkerware più utilizzato in base alle nostre statistiche 2020. Questo sample viene impiegato per vendere una gamma di diversi prodotti stalkerware come iSpyoo, TheTruthSpy e Copy9.
- A livello di diffusione geografica vediamo emergere una tendenza abbastanza coerente: Russia, Brasile e Stati Uniti restano i Paesi più colpiti a livello mondiale nel 2020.
- Il podio europeo dei Paesi più colpiti spetta rispettivamente a Germania, Italia e Regno Unito.



Introduzione e metodologia

La tecnologia ha consentito alle persone di connettersi come mai prima d'ora. Possiamo scegliere di condividere virtualmente la nostra vita con il partner, la famiglia e gli amici a prescindere dalla lontananza fisica. Tuttavia stiamo parallelamente assistendo a un incremento di software che consentono agli utenti di spiare in remoto la vita di un'altra persona tramite il proprio dispositivo, senza che l'utente interessato dia il proprio consenso o venga informato.

I rischi dello stalkerware possono superare la sfera virtuale e avere degli effetti nel mondo reale. La Coalition Against Stalkerware (Coalizione contro gli stalkerware) avverte che lo stalkerware "può facilitare la sorveglianza intima del partner, le molestie, gli abusi, lo stalking e/o la violenza".

Il software, noto come stalkerware, è disponibile in commercio a chiunque abbia accesso a Internet. I rischi dello stalkerware possono superare la sfera virtuale e avere degli effetti nel mondo reale. La Coalition Against Stalkerware (Coalizione contro gli stalkerware) avverte che lo stalkerware "può facilitare la sorveglianza intima del partner, le molestie, gli abusi, lo stalking e/o la violenza". Lo stalkerware può anche funzionare in modalità stealth, ovvero senza che sul dispositivo siano presenti delle icone che ne segnalino la presenza e restando quindi nascosto all'utente interessato. La maggior parte degli utenti colpiti non è nemmeno a conoscenza dell'esistenza di queste tipologie di software. Ciò significa che gli utenti non possono proteggersi, né online né offline, soprattutto perché chi fa uso degli stalkerware in genere conosce personalmente la vittima.

Negli ultimi anni Kaspersky ha collaborato attivamente con alcuni partner per porre fine all'uso degli stalkerware. Nel 2019 abbiamo creato uno speciale messaggio di allerta che segnala agli utenti se il software di stalkerware è installato sul proprio telefono. In seguito siamo diventati tra i dieci membri fondatori della Coalition Against Stalkerware. Nello stesso anno abbiamo anche pubblicato il nostro primo rapporto completo sullo stato dello stalkerware in modo da indagare la portata del problema.

Questo rapporto analizza il fenomeno dello stalkerware e presenta nuove statistiche per il 2020 rispetto ai dati rilevati l'anno precedente. I dati del rapporto sono stati ricavati da statistiche di minacce aggregate ottenute da Kaspersky Security Network. Kaspersky Security Network è un sistema dedicato all'elaborazione dei dati di sicurezza informatica inviati da milioni di partecipanti volontari in tutto il mondo. Tutti i dati ricevuti vengono resi anonimi. Il calcolo delle nostre statistiche si basa sull'analisi dellesoluzioni di sicurezza Kaspersky della linea consumer per dispositivi mobili.

Aspetti pratici e assetto storico dello stalkerware

Il software di sorveglianza stalkerware è disponibile in commercio a tutti coloro che abbiano accesso a Internet. Viene impiegato per spiare in remoto la vita di un'altra persona tramite il proprio dispositivo digitale senza che l'utente interessato dia il proprio consenso o venga informato. Lo stalkerware funziona in modalità stealth, ovvero senza che sul dispositivo siano presenti delle icone che ne segnalino la presenza. Resta quindi nascosto all'utente interessato. Di conseguenza la Coalition Against Stalkerware definisce lo stalkerware come un software che "può facilitare la sorveglianza intima del partner, le molestie, gli abusi, lo stalking e/o la violenza".

Dimensioni della cyberviolenza

In Europa, sette donne su dieci che hanno subito cyberstalking hanno subito anche almeno una forma di violenza fisica e/o sessuale da parte di un partner intimo.

Secondo un rapporto dell'Istituto europeo per l'uguaglianza di genere "in Europa, sette donne su dieci che hanno subito cyberstalking hanno subito anche almeno una forma di violenza fisica e/o sessuale da parte di un partner intimo". Sulla base di questi risultati gli esperti di organizzazioni non a scopo di lucro, che aiutano le vittime e le persone sopravvissute agli abusi domestici, sottolineano come il cyberstalking costituisca anche una forma di violenza. Proprio come nei casi di violenza fisica, psicologica ed economica il persecutore può servirsi della sorveglianza per ottenere e mantenere il controllo completo della propria vittima/sopravvissuto[1].

Attraverso lo stalkerware, il persecutore detiene una capacità di controllo potenzialmente immensa. A seconda del tipo di software installato, lo stalkerware può contare su una serie di funzioni che gli consentono di intromettersi nella vita privata della vittima. Con l'aiuto del softwareè possibile:

- Leggere tutto quello che viene digitato dalla persona sorvegliata e registrare ogni dato inserito nel dispositivo, comprese le credenziali di qualsiasi tipo di servizio come applicazioni bancarie, negozi online e social network, ecc.
- Scoprire dove si trova la persona tramite il monitoraggio in tempo reale dei movimenti con il GPS
- Ascoltare quello che viene detto tramite l'intercettazione delle chiamate, potendole persino registrare

1 Gli esperti si avvalgono sempre più spesso del termine "sopravvissuto" piuttosto che di "vittima". Pertanto in questa relazione useremo entrambi i termini.

- Leggere i messaggi su qualsiasi sistema di messaggistica a prescindere dall'uso di funzioni crittografiche
- Monitorare tutta l'attività sulle piattaforme social
- Guardare foto e video
- Accendere la fotocamera

Tutte queste informazioni private possono venire raccolte in genere da un dispositivo mobile come un tablet o uno smartphone.

Le organizzazioni senza scopo di lucro della Coalition Against Stalkerware stanno riscontrando la presenza di un numero crescente di sopravvissuti che cercano aiuto per risolvere il problema.

Le organizzazioni senza scopo di lucro della Coalition Against Stalkerware stanno riscontrando la presenza di un numero crescente di sopravvissuti che cercano aiuto per risolvere il problema:

- In base ai risultati del secondo sondaggio nazionale sull'abuso della tecnologia e sulla violenza domestica in **Australia**, lanciato da Rete di servizi per le donne in Australia (WESNET) e affiancato dalla dott.ssa Delanie Woodlock e dai ricercatori della Curtin University, il 99,3% dei professionisti che si occupano di violenza domestica ha clienti che subiscono abusi compiuti con l'ausilio della tecnologia. L'uso delle videocamere è aumentato inoltre del 183,2% tra il 2015 e il 2020.
- Secondo uno studio sulla cyberviolenza nelle relazioni intime, condotto dal Centre Hubertine Auclert in **Francia**, il 21% delle vittime ha subito episodi di stalkerware per mano del proprio partner violento e il 69% delle vittime sospetta che il partner abbia avuto accesso a informazioni personali presenti sul proprio smartphone in modo occulto.
- Da diversi anni in **Germania** i Centri di consulenza per donne e centri di crisi per lo stupro (bff) hanno rilevato l'impiego crescente di stalkerware nelle relazioni con il partner.
- Secondo lo Stalking Prevention Awareness & Resource Center negli **Stati Uniti** lo stalking colpisce circa 6-7,5 milioni di persone nell'arco di un anno e una vittima su quattro riferisce di essere stata perseguitata mediante una qualche forma di tecnologia.

L'accesso fisico come strumento chiave

Sfortunatamente non è difficile installare uno stalkerware sul dispositivo di una vittima a sua insaputa. La barriera principale riguarda la necessità di configurare lo stalkerware sul dispositivo preso di mira. A causa del vettore di distribuzione di tali applicazioni, che sono molto diverse dai comuni schemi di distribuzione di malware, è impossibile essere infettati da uno stalkerware tramite un messaggio di spam con un collegamento allo stalkerware o tramite la normale navigazione web.

Ciò significa che l'autore dell'abuso dovrà avere fisicamente accesso al dispositivo preso di mira per potere installare lo stalkerware. Questo è possibile se il dispositivo non dispone di pin, pattern di sblocco o password atte a proteggerlo oppure, in alternativa, quando il responsabile conosce personalmente la vittima/il sopravvissuto. L'installazione sul dispositivo interessato può essere completata in pochi minuti.

Prima di accedere al dispositivo del sopravvissuto, il persecutore deve ottenere il link al pacchetto di installazione dalla pagina web dello sviluppatore dello stalkerware. Nella maggior parte dei casi il software non viene scaricato da uno store di applicazioni ufficiale. Per quanto riguarda i dispositivi Android, nel 2020 Google ha bandito dallo store Google Play tutte le applicazioni che sono chiaramente stalkerware. Di conseguenza il perpetratore non è in grado di installare questo genere di applicazioni dall'App Store, ma è pertanto obbligato a seguire diversi passaggi prima di installare lo stalkerware. Ciò significa che potrebbe lasciare delle tracce nelle impostazioni del dispositivo, rintracciabili dalla vittima nel momento in cui questa sospetta di essere spiata.

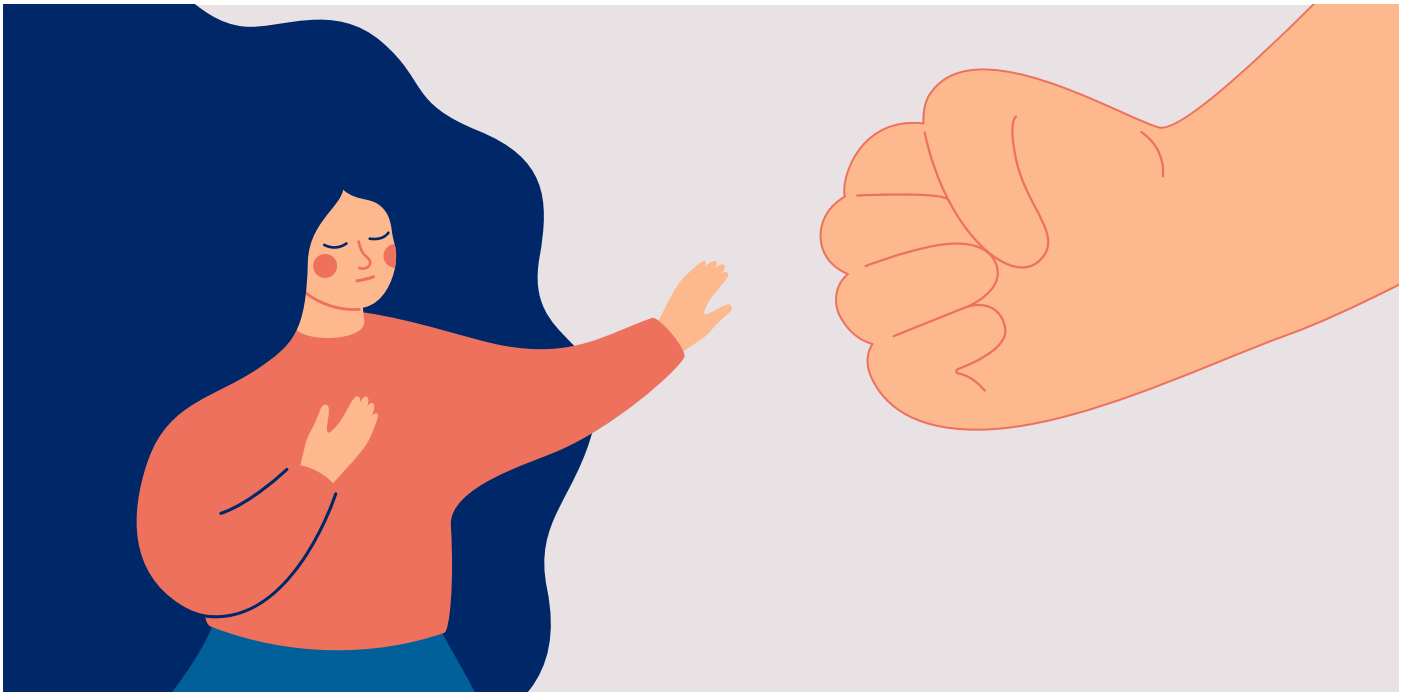
Gli strumenti dello stalkerware sono meno frequenti sugli iPhone che sui dispositivi Android.

Gli strumenti dello stalkerware sono meno frequenti sugli iPhone che sui dispositivi Android in quanto iOS è tradizionalmente un sistema chiuso. I fruitori possono però aggirare tale limitazione in tutti gli iPhone modificati tramite jailbreaking. Questo prevede comunque un accesso fisico al telefono per eseguire il jailbreak, pertanto gli utenti di iPhone che temono di essere sorvegliati dovrebbero sempre vigilare attentamente sul proprio dispositivo. Il persecutore può in alternativa offrire come regalo alla propria vittima un iPhone - o qualsiasi altro dispositivo - con uno stalkerware preinstallato. Molte aziende rendono disponibili i propri servizi online per installare tali strumenti su un nuovo telefono e consegnarlo nella confezione di fabbrica a un destinatario inconsapevole, ad esempio per celebrare un'occasione speciale.

Il rischio di diffusione dei dati personali

Le informazioni monitorate tramite lo stalkerware vengono rese disponibili ad almeno una persona, ovvero a colui che ha installato lo stalkerware sul telefono del sopravvissuto. Tuttavia a volte è possibile che tutti i dati privati possano diventare di dominio pubblico. Anno dopo anno i server stalkerware vengono violati o lasciati non protetti consentendo la consultazione e la diffusione delle informazioni online. Ad esempio, nel 2020 si è verificata una violazione dei dati su un prodotto fornito da ClevGuard. Negli anni precedenti abbiamo assistito a incidenti simili con Mobiispy nel 2019 e con MSpy nel 2018 e nel 2015.

Si tratta solo di alcuni esempi di una lunga lista in cui si documenta come i database di aziende che sviluppano stalkerware siano stati esposti, arrecando danno a milioni di account di utenti. La possibilità di tracciare la posizione di una persona significa non solo che la sua cyber-riservatezza è persa, ma anche la sua sicurezza nel mondo reale potrebbe essere a repentaglio.



Status giuridico

Le applicazioni stalkerware vengono vendute e fornite dalle aziende in varie forme, come sistemi di monitoraggio dei figli o soluzioni di tracciamento dei dipendenti. L'assetto legale varia tra i diversi Paesi e stati, ma le cose stanno cambiando. In generale si ritiene illegale solo l'impiego degli strumenti e app che registrano l'attività dell'utente senza il suo consenso o quello dell'autorità legale. Ma si stanno gradualmente registrando alcuni cambiamenti dal punto di vista legislativo. Ad esempio, nel 2020 la Francia ha inasprito le sanzioni sulla sorveglianza segreta: geolocalizzare qualcuno senza il suo consenso è ora punibile con un anno di reclusione e una multa di 45.000 euro. Se ciò avviene all'interno di una coppia le sanzioni sono potenzialmente più alte, potendo includere due anni di reclusione e una multa di 60.000 euro.

Gli strumenti di stalkerware spesso violano le leggi ed espongono il persecutore a responsabilità legali per una qualsiasi registrazione eseguita all'insaputa della vittima. I persecutori devono rendersi conto di trovarsi in condizioni di violazione della legge. In seguito alla segnalazione di stalkerware la sanzione viene inflitta all'autore privato che ha installato il software e non al venditore. Nella storia recente degli Stati Uniti sono soltanto due gli sviluppatori di app di stalking multati. Uno ha dovuto pagare la multa record di 500.000 dollari, che ha posto fine al processo di sviluppo dell'app, mentre l'altro è stato costretto a modificare la funzionalità dell'app per le vendite future.

La portata del problema

Dati complessivi di rilevamento – utenti interessati

Nel 2020 erano in totale 53.870 gli utenti unici vittime di stalkerware a livello mondiale, mentre nel 2019 gli utenti unici vittime di stalkerware a livello mondiale erano 67.500.

In questa sezione viene esaminato il numero complessivo di utenti unici il cui dispositivo mobile è stato scoperto essere soggetto a stalkerware.

I dati del 2020 mostrano che la situazione dello stalkerware non è migliorata di molto e il numero delle persone colpite resta alto. Nel 2020 erano in totale 53.870 gli utenti unici vittime di stalkerware a livello mondiale, mentre nel 2019 gli utenti unici vittime di stalkerware a livello mondiale erano 67.500. Occorre tuttavia tenere conto del fatto che il 2020 è stato un anno senza precedenti, con cambiamenti drammatici nello stile di vita registrati in ogni parte del mondo.

Per combattere la pandemia di COVID-19, tutti i Paesi del mondo hanno dovuto affrontare enormi restrizioni, quali le misure di autoisolamento o gli obblighi di confinamento, per

far restare le persone a casa. Considerando che lo stalkerware viene utilizzato come strumento aggiuntivo per controllare un partner intimo con cui il persecutore convive nella vita quotidiana, tale circostanza è in grado di spiegare i numeri leggermente inferiori rispetto all'anno precedente.

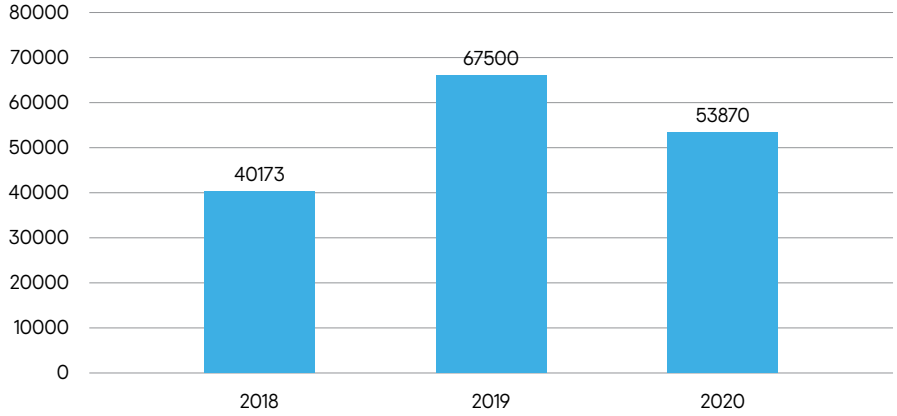


Tabella 1 Utenti unici interessati dallo stalkerware a livello mondiale dal 2018 al 2020 – totale annuo

Si evince, dunque, che i numeri del 2020 permangono stabilmente su un livello elevato. In confronto, nel 2018 si sono registrati 40.173 casi di utenti unici colpiti a livello mondiale dallo stalkerware.

Osservando le cifre del numero totale di utenti unici interessati dallo stalkerware nel 2020 nel mondo, in un mese, tale tendenza diventa ancora più evidente. I primi due mesi dell'anno si sono rivelati stabili, con un aumento apprezzabile di dispositivi colpiti a dimostrazione di una certa popolarità del fenomeno stalkerware. La situazione è cambiata nel mese di marzo, quando molti Paesi hanno deciso di mettere in atto le misure di quarantena. La curva mostra una tendenza secondo cui i numeri hanno iniziato a stabilizzarsi a partire da giugno 2020, nel momento in cui molti Paesi in tutto il mondo hanno allentato le restrizioni. .

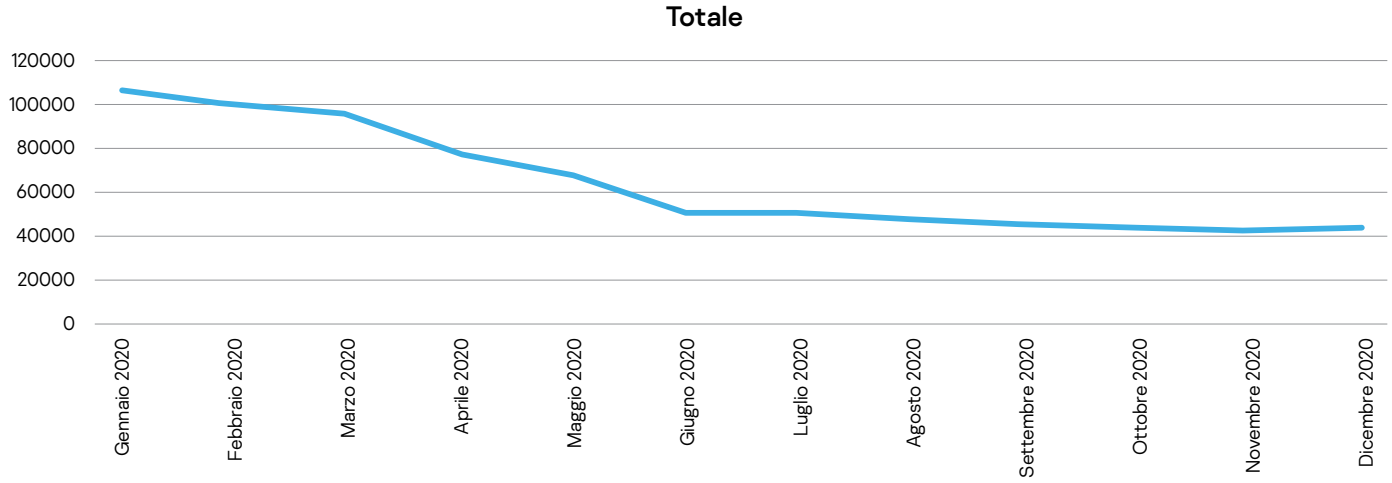


Tabella 2 Utenti unici interessati dallo stalkerware a livello mondiale nel 2020 – per mese

Si evince, dunque, che i numeri del 2020 permangono stabilmente su un livello elevato. In confronto, nel 2018 si sono registrati 40.173 casi di utenti unici colpiti a livello mondiale dallo stalkerware. Ciò porta ad analizzare in prospettiva i numeri totali del 2020, considerando la crescente irruzione tecnologica nelle nostre vite. Purtroppo questo significa anche che il software utilizzato per lo stalking sta diventando un'ulteriore forma di violenza sempre più comune perpetrata dal partner.

Dati complessivi di rilevamento – sample di stalkerware

In questa sezione vengono analizzati i sample di stalkerware più utilizzati per controllare i dispositivi mobili su base complessiva. Nel 2020 i sample più rilevati possono essere osservati nei seguenti risultati:

	Sample	Utenti colpiti
1	Monitor.AndroidOS.Nicb.a	8147
2	Monitor.AndroidOS.Cerberus.s	5429
3	Monitor.AndroidOS.Agent.af	2727
4	Monitor.AndroidOS.Anlost.a	2234
5	Monitor.AndroidOS.MobileTracker.c	2161
6	Monitor.AndroidOS.PhoneSpy.b	1774
7	Monitor.AndroidOS.Agent.hb	1463
8	Monitor.AndroidOS.Cerberus.a	1310
9	Monitor.AndroidOS.Reptilic.a	1302
10	Monitor.AndroidOS.SecretCam.a	1124

Tabella 3 – I primi 10 sample di stalkerware più rilevati a livello mondiale nel 2020osservati nei seguenti risultati:

1. Con oltre 8.100 utenti colpiti, **Nidb** risulta essere il sample di stalkerware più utilizzato nel 2020. Il creatore di Nidb vende il proprio prodotto come Stalkerware-as-a-Service. Ciò significa che chiunque può noleggiare il software e l'applicazione mobile sul server di controllo, ridefinirli con un nome commerciale adatto e venderli separatamente: alcuni esempi includono iSpyoo, TheTruthSpy, Copy9 e altri.
2. Il secondo e l'ottavo posto sono detenuti da Cerberus. Si tratta di due sample diversi della stessa famiglia. La versione **Cerberus.a** ha interessato più di 5.400 utenti.
3. Con oltre 2.700 utenti colpiti, **Agent.af** ricopre la terza posizione. Il prodotto è commercializzato come Track My Phone e possiede funzionalità classiche come la lettura dei messaggi da qualsiasi sistema di messaggistica, la registrazione della cronologia delle chiamate e il tracciamento della geolocalizzazione.
4. **Anlost.a** costituisce un buon esempio di stalkerware in incognito. Viene pubblicizzata come applicazione antifurto e l'icona appare nella schermata principale (comportamento non usuale per un'app stalkerware nascosta). Di conseguenza è disponibile su Google Play Store. Ciò detto, è possibile nascondere deliberatamente l'icona dalla schermata principale. Una delle funzionalità chiave dell'applicazione riguarda l'intercettazione degli SMS e la lettura del registro delle chiamate. Oltre 2.200 utenti sono stati vittima di questo sample.
5. **MobileTracker.c** possiede diverse funzionalità, quali l'intercettazione dei messaggi dai social network più diffusi e l'assunzione del controllo remoto del dispositivo interessato. Oltre 2.100 utenti sono stati vittima di questo sample.
6. **PhoneSpy** è noto anche come app Spy Phone o Spapp Monitoring. Questa applicazione è composta da molte funzionalità spia che coprono tutti i programmi di messaggistica istantanea e i social network più popolari.
7. **Agent.hb** è un'altra versione di MobileTracker. Come la versione originale, offre molte funzionalità.
8. **Cerberus.b** è un sample diverso appartenente alla stessa famiglia di Cerberus.a.
9. **Reptilic.a** è uno stalkerware che include molte funzionalità, quali il monitoraggio dei social media, la registrazione delle chiamate e il monitoraggio della cronologia del browser.
10. **SecretCam.a** è un software di stalking della fotocamera. È quindi in grado di registrare segretamente dei filmati dalla fotocamera anteriore o posteriore del dispositivo interessato.

Geografica degli utenti colpiti

Lo stalkerware è un fenomeno globale che colpisce i Paesi indipendentemente dalle dimensioni, dal tipo di società o dalla cultura. Esaminando i primi 10 Paesi colpiti in tutto il mondo nel 2020, i risultati di Kaspersky mostrano che i Paesi più colpiti sono gli stessi, con la Russia al primo posto. Rispetto al 2019, nel corso del 2020 si assiste tuttavia a un aumento dell'attività di stalkerware in Brasile e negli Stati Uniti. Si registrano invece meno incidenti in India, Paese sceso di posizione. Abbiamo inoltre rilevato un numero maggiore di incidenti in Messico, salito di due posti nella classifica.

	Paese	Utenti colpiti
1	Federazione Russa	12389
2	Brasile	6523
3	Stati Uniti d'America	4745
4	India	4627
5	Messico	1570
6	Germania	1547
7	Iran	1345
8	Italia	1144
9	Regno Unito	1009
10	Arabia Saudita	968

Tabella 4 – I primi 10 Paesi maggiormente colpiti da stalkerware a livello mondiale nel 2020

Se si considera l'Europa, Germania, Italia e Regno Unito sono, nell'ordine, i tre Paesi più colpiti. Seguono la Francia al quarto posto e la Spagna al quinto.

	Paese	Utenti colpiti
1	Germania	1547
2	Italia	1144
3	Regno Unito	1009
4	Francia	904
5	Spagna	873
6	Polonia	444
7	Paesi Bassi	321
8	Romania	222
9	Belgio	180
10	Austria	153

Tabella 5 – I primi 10 Paesi più colpiti dallo stalkerware a livello europeo nel 2020

Come verificare se sul dispositivo mobile è installato uno stalkerware

A un utente che utilizza quotidianamente il telefono risulta difficile sapere se è stato installato uno stalkerware sul proprio dispositivo. Questo tipo di software resta in genere occulto: si cela l'icona dell'app stalkerware nella schermata iniziale e nel menu del telefono si elimina persino qualsiasi traccia lasciata. Tuttavia, potrebbe manifestarsi attraverso alcuni segnali di pericolo. Tra i segnali più rilevanti e le azioni da intraprendere possiamo trovare:

- Batteria che si scarica rapidamente, surriscaldamento costante e crescita del traffico dati sul dispositivo mobile.
- Eseguire regolarmente scansioni antivirus sui dispositivi Android: se la funzionalità di sicurezza informatica ha rilevato uno stalkerware **non affrettarsi a rimuoverlo in quanto il maltrattante potrebbe accorgersene**. Predisporre un piano di sicurezza e contattare una struttura di assistenza locale.
- Controllare la cronologia del browser: per scaricare lo stalkerware il persecutore deve visitare alcune pagine web di cui l'utente interessato non è a conoscenza. Se il persecutore la elimina, però, non risulterà presente nella cronologia.
- Controllare le impostazioni di "fonti sconosciute": l'abilitazione di "fonti sconosciute" sul dispositivo può segnalare la presenza di software indesiderato installato da fonti di terze parti.
- Controllare le autorizzazioni delle app installate: l'applicazione stalkerware potrebbe celarsi dietro a un nome diverso e avere sospetto a messaggi, registri chiamate, posizione e altre attività personali.

Resta tuttavia importante comprendere che i segnali di pericolo o i sintomi non costituiscono necessariamente una prova di installazione dello stalkerware su un dispositivo.

In contesti di violenza domestica e relazioni abusanti può essere difficile, quando non impossibile, negare al partner violento l'accesso al telefono.

Come minimizzare il rischio

Di seguito si indicano alcuni consigli utili a incrementare la sicurezza digitale:

- Non prestare mai il telefono a nessuno senza vedere che uso ne viene fatto e non lasciarlo mai sbloccato.*
- Ricorrere a una password complessa sulla schermata di blocco e modificare regolarmente le password.
- Non rivelare la propria password a nessuno, nemmeno al partner intimo, ai familiari o agli amici stretti.*
- Eseguire controlli regolari del telefono: eliminare le app che non vengono utilizzate e controllare le autorizzazioni concesse a ciascuna app.
- Disabilitare l'opzione di installazione di applicazioni di terze parti sui dispositivi Android.
- Proteggere i dispositivi Android con una funzionalità di sicurezza informatica come Kaspersky Internet Security per Android (gratuito) che rileva lo stalkerware e notifica degli avvisi.

*In contesti di violenza domestica e relazioni abusanti può essere difficile, quando non impossibile, negare al partner violento l'accesso al telefono.

Le attività e il contributo di Kaspersky per porre fine alla cyberviolenza

Kaspersky sta lavorando attivamente per porre fine all'uso di cyberviolenza e stalkerware in qualità di azienda e congiuntamente a molti altri partner. Nel 2019 abbiamo creato un avviso ad hoc che segnala agli utenti se il software di stalkerware è installato sul telefono. Nello stesso anno, con altri nove membri fondatori, abbiamo creato l'organizzazione Coalition Against Stalkerware. Nel 2020 abbiamo prodotto TinyCheck, uno strumento gratuito per rilevare lo stalkerware sui dispositivi mobili dedicato in particolare alle organizzazioni di servizi che lavorano con vittime di violenza domestica. TinyCheck è disponibile su https://github.com/KasperskyLab/TinyCheck. Dal 2021 siamo uno dei cinque partner di un progetto a livello dell'UE volto a contrastare la cyberviolenza e lo stalkerware di genere chiamato DeStalk, che la Commissione europea ha scelto di sostenere con il programma Diritti, Uguaglianza e Cittadinanza.

Informazioni su Coalition Against Stalkerware

La Coalition Against Stalkerware ("CAS" o "Coalizione") è un gruppo dedicato al contrasto di abusi, stalking e molestie attraverso la creazione e l'uso di stalkerware. Lanciato a novembre 2019, il gruppo Coalition Against Stalkerware ha visto la partecipazione di 26 partner nel primo anno. Questi includono partner fondatori come: Avira, Electronic Frontier Foundation, the European Network for the Work with Perpetrators of Domestic Violence, G DATA Cyber Defense, Kaspersky, Malwarebytes, The National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape e WEISSER RING. La Coalizione cerca di riunire un'ampia gamma di organizzazioni per affrontare attivamente il comportamento criminale perpetrato attraverso lo stalkerware e aumentare la consapevolezza del pubblico riguardo a questo importante problema. A causa dell'elevata rilevanza sociale per gli utenti in tutto il mondo e delle nuove varianti di stalkerware che emergono periodicamente, il gruppo Coalition Against Stalkerware è aperto a nuovi partner e fa appello a ulteriori collaborazioni. Per saperne di più su Coalition Against Stalkerware, visitare il sito ufficiale https://stopstalkerware.org/it.