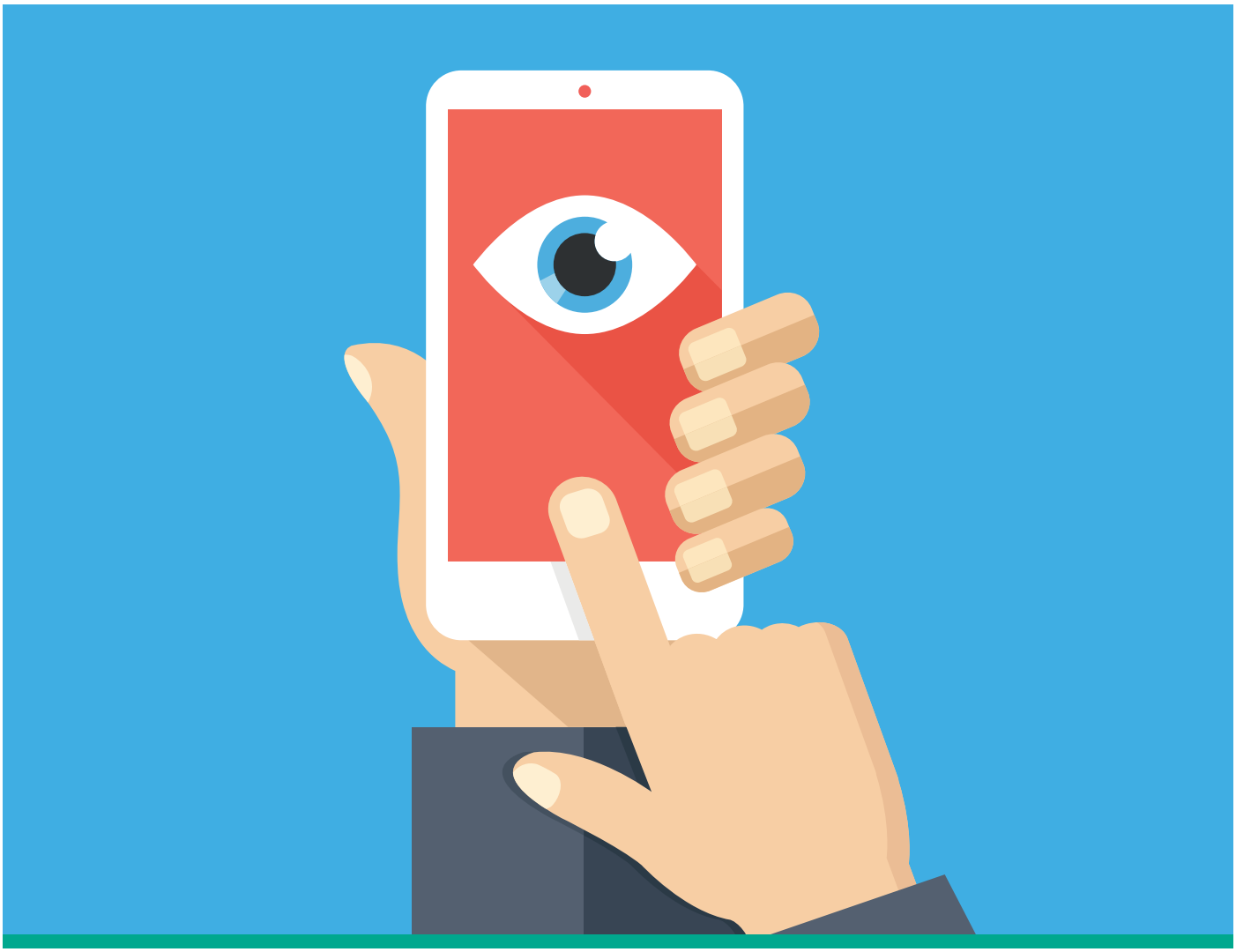


Le point sur les **stalkerwares** en 2020

COALITION AGAINST STALKERWARE

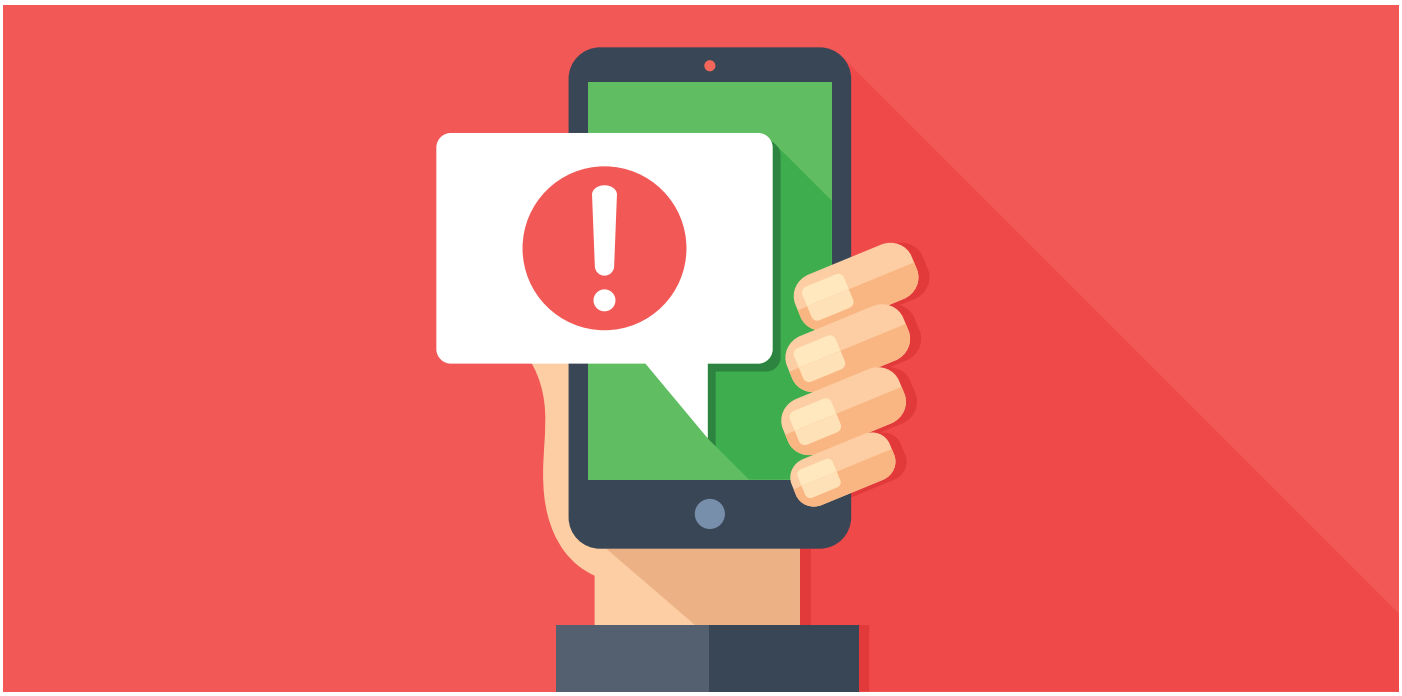
kaspersky

Sommaire

Principaux constats 2020

Les données de Kaspersky indiquent que l'ampleur du phénomène des stalkerwares ne s'est guère amoindrie en 2020 par rapport à l'année précédente :

- Le nombre de personnes touchées reste élevé. Au total, parmi nos utilisateurs mobiles, 53 870 ont été affectés par un stalkerware en 2020. Ces chiffres n'incluant que les utilisateurs Kaspersky, il est important de souligner que les valeurs totales réelles sont plus élevées. Certains utilisateurs touchés par ce problème peuvent utiliser une autre solution de cybersécurité sur leurs appareils, tandis que d'autres n'en utilisent encore aucune.
- Avec plus de 8 100 utilisateurs affectés à l'échelle mondiale, selon nos statistiques 2020, Nidb est l'échantillon de stalkerware le plus répandu. Cet échantillon est utilisé pour vendre divers produits de harcèlement, tels que iSpyoo, TheTruthSpy et Copy9, pour ne citer qu'eux.
- En matière de répartition géographique, une tendance constante semble se dessiner : la Russie, le Brésil et les États-Unis restent les trois pays les plus touchés à l'échelle mondiale en 2020.
- En Europe, l'Allemagne, l'Italie et le Royaume-Uni sont respectivement les trois pays les plus affectés.



Introduction et méthodologie

La technologie permet aujourd'hui aux individus de rester plus que jamais connectés. Grâce au numérique, nous pouvons choisir de partager notre vie avec notre conjoint, notre famille, nos amis, où qu'ils se trouvent dans le monde. Néanmoins, nous constatons également une hausse des logiciels permettant d'espionner à distance la vie d'autres personnes à travers leurs appareils numériques, sans qu'elles aient donné leur consentement ou qu'elles en aient été averties.

Les risques liés aux stalkerwares ne se limitent pas à la sphère du virtuel, mais touchent également le monde physique. La Coalition contre les stalkerwares avertit que ces logiciels « peuvent faciliter et favoriser la surveillance, le harcèlement, la maltraitance et/ou la violence envers les conjoints ».

Ces logiciels, appelés stalkerwares, sont disponibles à l'achat à toute personne disposant d'un accès à Internet. Les risques liés aux stalkerwares ne se limitent pas à la sphère du virtuel, mais touchent également le monde physique. La Coalition contre les stalkerwares avertit que ces logiciels « peuvent faciliter et favoriser la surveillance, le harcèlement, la maltraitance et/ou la violence envers les conjoints ». Les stalkerwares, ou logiciels espions, peuvent également fonctionner en toute discrétion, ce qui signifie qu'aucune icône n'est affichée sur l'appareil de l'utilisateur pour en révéler la présence. Les utilisateurs touchés, pour la plupart, ne sont même pas conscients de l'existence de tels logiciels. Il leur est donc impossible de s'en protéger, en ligne ou hors ligne, en particulier parce que le plus souvent, l'utilisateur du stalkerware connaît sa victime personnellement.

Depuis quelques années, Kaspersky collabore activement avec différents partenaires pour contrer l'utilisation des stalkerwares. En 2019, nous avons créé au sein de nos solutions de sécurité, une alerte spéciale qui avertit les utilisateurs lorsqu'un stalkerware est installé sur leur téléphone. Suite à cela, nous sommes devenus l'un des dix membres fondateurs de la Coalition contre les stalkerwares. La même année, nous avons également publié notre premier rapport complet faisant le point sur les stalkerwares, pour appréhender l'ampleur du problème.

Le présent rapport poursuit l'analyse de ce problème et présente de nouvelles statistiques issues de l'année 2020, en comparaison avec nos données précédentes. Les données du présent rapport se fondent sur les statistiques agrégées des menaces générées fournies par Kaspersky Security Network. Kaspersky Security Network se consacre au traitement des flux de données de cybersécurité provenant de millions de participants volontaires à travers le monde. Toutes les données reçues sont anonymisées. Pour le calcul de nos statistiques, nous consultons la gamme grand public de solutions de sécurité mobile Kaspersky.

Les stalkerwares : problème et historique

Les logiciels espions, ou stalkerwares, sont disponibles à l'achat à toute personne disposant d'un accès à Internet. Ils permettent d'espionner à distance la vie d'autres personnes à travers leurs appareils, sans qu'elles aient donné leur consentement ou qu'elles en aient été averties. Les stalkerwares fonctionnent en toute discrétion, ce qui signifie qu'aucune icône n'est affichée sur l'appareil de l'utilisateur pour en révéler la présence. C'est pourquoi, selon la définition de la Coalition contre les stalkerwares, les stalkerwares sont les logiciels « capables de faciliter et de favoriser la surveillance, le harcèlement, la maltraitance et/ou la violence envers les conjoints ».

La dimension des cyberviolences

7 femmes sur 10 en Europe touchées par le cyberharcèlement ont également été victimes d'une forme de violence physique et/ou sexuelle de la part de leur conjoint.

Selon un rapport établi par l'Institut européen pour l'égalité entre les hommes et les femmes, « 7 femmes sur 10 en Europe touchées par le cyberharcèlement ont également été victimes d'une forme de violence physique et/ou sexuelle de la part de leur conjoint ». En résonance avec ces constatations, des experts d'associations à but non lucratif (ABNL) venant en aide aux victimes/rescapés de maltraitances conjugales rappellent que le cyberharcèlement est également une forme de violence. Au même titre que la violence physique, psychologique ou économique, un agresseur peut utiliser la surveillance pour contrôler complètement les victimes/rescapés[1] et garder la main sur la situation.

Au moyen d'un stalkerware, un agresseur peut obtenir une forme de contrôle d'une étendue considérable. Les différents types de stalkerwares peuvent proposer de nombreuses fonctions pour s'immiscer dans la vie privée des victimes. Au moyen d'un tel logiciel, un agresseur peut :

- Lire tout ce que la personne surveillée écrit : chaque pression sur une touche de l'appareil est enregistrée, y compris les données d'identification à des services bancaires, sites d'achats en ligne, aux réseaux sociaux, etc.
- Savoir où se trouve la victime, dont les mouvements sont tracés en temps réel à l'aide du GPS.
- Écouter et même enregistrer toutes les conversations de la personne surveillée.
- Lire tous les messages (SMS, messagerie), quel que soit le chiffrement utilisé.
- Contrôler l'activité sur les réseaux sociaux.

1 Les experts, plutôt que de parler de « victimes », tendent à utiliser de plus en plus le terme « rescapés ». Dans ce rapport, nous utiliserons indifféremment ces deux termes.

- Voir les photos et les vidéos.
- Activer l'appareil photo.

Toutes ces informations privées peuvent être récupérées, généralement sur un appareil mobile comme une tablette ou un smartphone.

Les associations à but non lucratif de la Coalition contre les stalkerwares sont contactées par un nombre grandissant de victimes cherchant de l'aide.

Les associations à but non lucratif de la Coalition contre les stalkerwares sont contactées par un nombre grandissant de victimes cherchant de l'aide :

- La Deuxième enquête nationale sur la violence conjugale et les maltraitances technologiques en **Australie**, initiée par le Réseau des services aux femmes en Australie (WESNET) avec l'aide du Dr Delanie Woodlock et de chercheurs de l'Université Curtin, révèle que 99,3 % des praticiens s'occupant de violences conjugales indiquent avoir des patients victimes d'abus liés aux technologies. Ces abus impliquant l'usage de caméras vidéo ont augmenté de 183,2 % entre 2015 et 2020.
- Selon une étude sur la cyberviolence dans les relations conjugales, réalisée par le Centre Hubertine Auclert en **France**, 21 % des victimes ont subi les méfaits des stalkerwares des mains de leur conjoint agresseur, et 69 % des victimes ont l'impression que les informations personnelles sur leurs smartphones ont été consultées en cachette par leur partenaire.
- En **Allemagne**, depuis plusieurs années, les centres de conseils aux femmes et d'aide aux victimes de viol (bff) remarquent une utilisation croissante des stalkerwares dans le cadre des relations conjugales.
- Aux **États-Unis**, le harcèlement a touché entre 6 et 7,5 millions de personnes sur la dernière année, et une victime sur quatre déclare avoir subi du harcèlement au moyen de technologies, selon le SPARC (Stalking Prevention Awareness & Resource Center).

L'accès physique à la source du problème

Malheureusement, il n'est guère compliqué d'installer secrètement un stalkerware sur le téléphone d'une personne. La seule contrainte réside dans la configuration nécessaire du stalkerware sur l'appareil visé. En raison du vecteur de distribution de telles applications, très différent des schémas habituels de distribution des malwares, il est impossible d'être infecté par un stalkerware à distance, par le biais d'un message indésirable comprenant un lien vers le logiciel ou par une session de navigation classique sur Internet.

Cela signifie que l'agresseur doit avoir accès physiquement à l'appareil ciblé pour installer le stalkerware. Cet accès est possible si l'appareil ne dispose d'aucune protection (code PIN, motif, mot de passe) ou si l'agresseur connaît personnellement la victime (et par conséquent ses codes confidentiels, mots de passe et/ou peut accéder à son empreinte digitale). L'installation sur l'appareil ciblé peut s'effectuer en quelques minutes.

Avant d'accéder à l'appareil de la victime, l'agresseur doit récupérer un lien vers le package d'installation sur la page Web du développeur du stalkerware. La plupart du temps, le logiciel n'est pas téléchargé depuis un magasin d'applications officiel. En effet, pour éviter que ce type de logiciel ne soit accessible via les plateformes de téléchargement officielles, Google a suspendu les applications identifiées clairement comme stalkerwares sur Google Play Store en 2020, pour les appareil Android. Pour y parvenir, l'agresseur devra suivre plusieurs étapes avant d'être en mesure d'installer le logiciel. De cette façon, l'agresseur peut laisser des traces dans les paramètres de l'appareil, qu'un utilisateur peut consulter s'il se sent espionné.

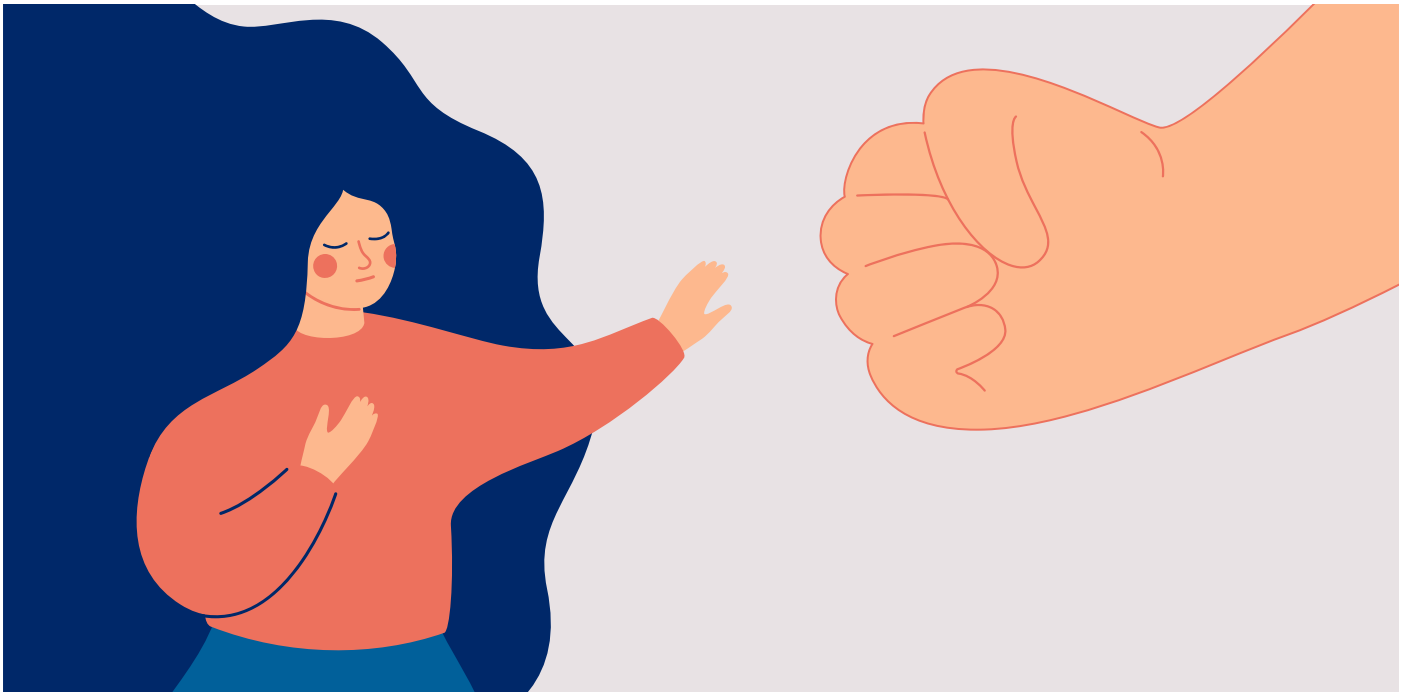
Les logiciels de harcèlement sont moins fréquents sur iPhone que sur Android.

Les logiciels de harcèlement sont moins fréquents sur iPhone que sur Android, car iOS est un système traditionnellement fermé. Toutefois, à condition d'avoir également accès au téléphone les agresseurs peuvent contourner la limitation d'Apple en débridant les iPhones. Les utilisateurs d'iPhone craignant une surveillance doivent donc garder un œil sur leur appareil à chaque instant. Certains agresseurs offrent également directement des smartphones déjà équipés d'un stalkerware. Un certain nombre d'entreprises, parfois peu scrupuleuses proposent d'ailleurs leurs services pour installer certains logiciels, comme des stalkerwares par exemple, sur un téléphone neuf, qui sera alors remis dans son emballage d'origine avant d'être livré en cadeau à un utilisateur non averti, qui deviendra victime.

Le risque de fuites de données confidentielles

Les informations surveillées par un stalkerware seront accessibles à un tiers, à minima celui qui a installé le logiciel (l'agresseur) sur le téléphone de la victime. Toutefois, il arrive aussi que les données privées soient également rendues publiques. Les serveurs des stalkerwares sont parfois piratés ou non protégés, et leurs informations peuvent être récupérées et diffusées en ligne. Par exemple, en 2020, une fuite de données de ce type est survenue en raison d'un produit proposé par ClevGuard. Les années précédentes, nous avons constaté d'autres incidents similaires : Mobiispy en 2019 ou encore MSpy en 2018 et 2015.

Il ne s'agit que de quelques exemples parmi de nombreux autres. Les bases de données des sociétés développant des stalkerwares ont été diffusées à maintes occasions, affectant des millions d'utilisateurs qui se retrouvent alors face à un double problème de confidentialité. Un utilisateur peut alors à son insu, non seulement être espionné par une personne de son entourage, mais également par des tas d'inconnus. La géolocalisation d'une personne à son insu compromet sa vie privée, mais peut également constituer un danger réel dans le monde physique.



Statut juridique

Les stalkerwares sont commercialisés et proposés par des sociétés œuvrant sous différentes couvertures, comme la surveillance des enfants ou des employés. Si les lois varient d'un pays à l'autre, elles tendent à s'harmoniser. De façon générale, seule est interdite l'utilisation des outils et applications qui enregistrent l'activité d'utilisateurs sans leur consentement ou l'autorisation d'un pouvoir légal. Nous constatons toutefois que les lois commencent à évoluer. Par exemple, en 2020, la France a renforcé les sanctions à l'encontre de la surveillance secrète : géolocaliser une personne sans son consentement est désormais passible d'un an d'emprisonnement et d'une amende de 45 000 euros. Si cette surveillance est effectuée au sein d'un couple, les sanctions sont potentiellement plus fortes, avec une peine d'emprisonnement allant jusqu'à deux ans et une amende de 60 000 euros.

Les stalkerwares enfreignent souvent les lois en vigueur et engagent la responsabilité légale du contrevenant en cas de surveillance effectuée sans le consentement de la victime. Les personnes utilisant de tels logiciels doivent comprendre qu'ils enfreignent la loi. Si l'utilisation d'un stalkerware est constatée, la sanction s'applique à la personne ayant installé le logiciel et non à son fournisseur. Récemment aux États-Unis, deux développeurs de stalkerwares ont néanmoins été sanctionnés. Le premier a dû s'acquitter d'une amende de 500 000 USD qui a mis fin au processus de développement de l'application, et le deuxième a dû modifier la fonctionnalité de l'application avant de pouvoir continuer à la commercialiser.

L'ampleur du problème

Chiffres de détection dans le monde – utilisateurs affectés

Au total, 53 870 utilisateurs dans le monde ont été victimes d'un stalkerware en 2020. En 2019, ce nombre s'élevait à 67 500 utilisateurs dans le monde.

Dans cette section, nous nous intéressons aux nombres d'utilisateurs sur l'appareil desquels des stalkerwares ont été détectés.

Les données 2020 indiquent que la situation en matière de stalkerwares ne s'est guère améliorée : le nombre de personnes affectées reste élevé. Au total, 53 870 utilisateurs dans le monde ont été victimes d'un stalkerware en 2020. En 2019, ce nombre s'élevait à 67 500 utilisateurs dans le monde. Toutefois, il est important de tenir compte du caractère exceptionnel de l'année 2020, où de nombreuses personnes ont vu leur vie changer radicalement.

En effet pour lutter contre la pandémie de COVID-19, tous les pays ont imposé d'importantes restrictions, comme les mesures de confinement ou de couvre-feu, pour obliger les gens à rester chez eux. Etant donné que les stalkerwares sont utilisés par l'agresseur pour contrôler la vie d'un conjoint dans sa vie quotidienne hors du domicile, les conditions de vie particulières de l'année 2020 peuvent expliquer en partie la baisse des chiffres par rapport à l'année précédente.

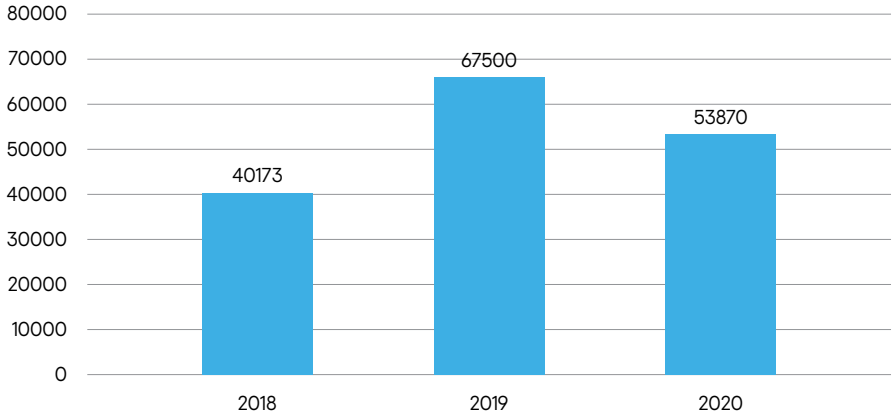


Table 1 - Nombre d'utilisateurs différents affectés par les stalkerwares dans le monde, de 2018 à 2020– total annuel

Lorsque nous regardons les chiffres du nombre total d'utilisateurs affectés mensuellement par des stalkerwares en 2020 à travers le monde, cette tendance est encore plus marquée.

Lorsque nous regardons les chiffres du nombre total d'utilisateurs affectés mensuellement par des stalkerwares en 2020 à travers le monde, cette tendance est encore plus marquée. Les deux premiers mois de l'année ont été stables, avec de nombreux nouveaux cas, reflétant la popularité des stalkerwares. La situation a évolué en mars, lorsque de nombreux pays ont annoncé des mesures de confinement. La courbe se stabilise au mois de juin 2020, alors que de nombreux pays commençaient à assouplir les contraintes.

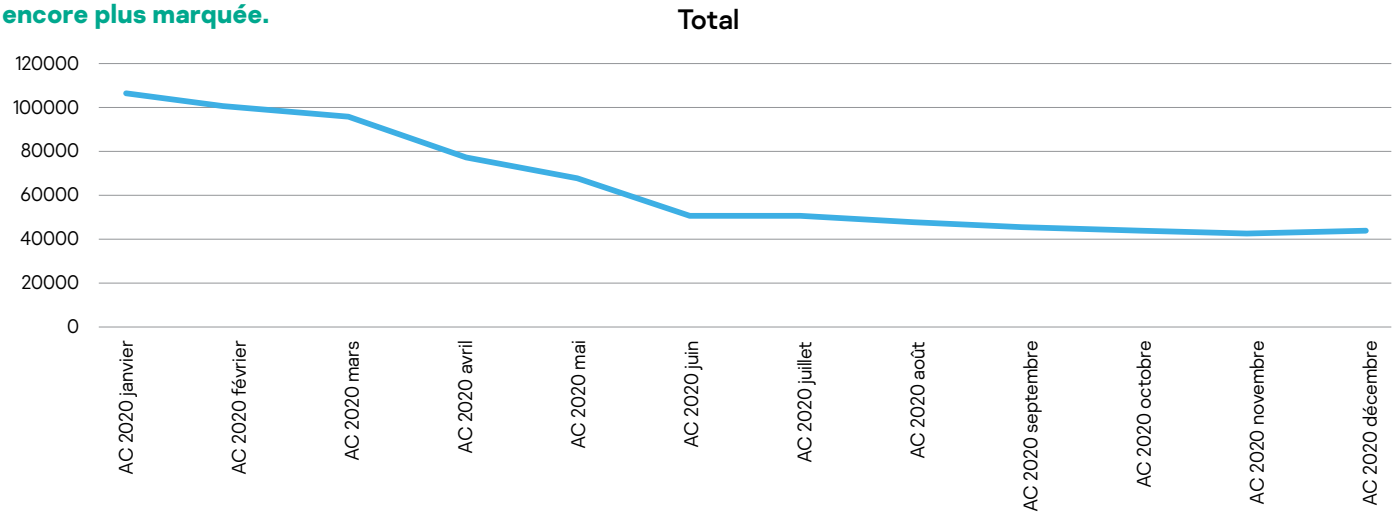


Table 2 – Nombre d'utilisateurs différents affectés par les logiciels de traque en 2020 dans le monde – total mensuel

Cela dit, les chiffres de 2020 restent à un niveau élevé et stable. En comparaison, en 2018, un stalkerware a été détecté chez 40 173 utilisateurs dans le monde. Ceci met en perspective les chiffres globaux de 2020, car nous avons constaté une intégration grandissante de la technologie dans nos vies. Malheureusement, cela démontre également que les stalkerwares ont gagné en importance et fréquence dans le cadre des violences conjugales.

Chiffres de détection dans le monde – échantillons de stalkerwares

Dans cette section, nous analysons les échantillons de stalkerwares les plus utilisés pour surveiller les appareils mobiles à échelle mondiale. Les échantillons les plus souvent détectés en 2020 sont présentés dans les résultats suivants :

	Échantillons	Utilisateurs affectés
1	Monitor.AndroidOS.Nicb.a	8 147
2	Monitor.AndroidOS.Cerberus.s	5 429
3	Monitor.AndroidOS.Agent.af	2 727
4	Monitor.AndroidOS.Anlost.a	2 234
5	Monitor.AndroidOS.MobileTracker.c	2 161
6	Monitor.AndroidOS.PhoneSpy.b	1 774
7	Monitor.AndroidOS.Agent.hb	1 463
8	Monitor.AndroidOS.Cerberus.a	1 310
9	Monitor.AndroidOS.Reptilic.a	1 302
10	Monitor.AndroidOS.SecretCam.a	1 124

Table 3 – Top 10 des échantillons de stalkerwares détectés en 2020 dans le monde

1. Avec plus de 8 100 utilisateurs affectés, **Nidb** est l'échantillon de stalkerware le plus répandu en 2020. Le créateur de Nidb vend son produit en tant que Stalkerware as a Service. Cela signifie que n'importe qui peut louer leur logiciel serveur et application mobile de contrôle, en changer le nom, puis revendre le produit. iSpyoo, TheTruthSpy, Copy9 (et d'autres) en sont des exemples.
2. Les deuxièmes et huitièmes places sont occupées par Cerberus. Cette même famille comprend deux échantillons différents. La variante **Cerberus.a** a affecté plus de 5 400 utilisateurs.
3. **Agent.af** arrive en troisième position, avec plus de 2 700 utilisateurs affectés. Ce logiciel est vendu sous le nom Track My Phone et présente des fonctions comme la lecture des messages de n'importe quelle messagerie, la consignation de l'historique des appels téléphoniques et le suivi de géolocalisation.
4. **Anlost.a** est un bon exemple de stalkerware masqué. Vendue comme une application antivol, son icône est présente sur l'écran d'accueil (ce qui n'est pas courant dans le monde généralement discret des logiciels de harcèlement). Ce logiciel est donc disponible dans Google Play Store. Cela dit, il est possible de masquer délibérément l'icône de l'écran d'accueil. L'une des fonctionnalités clés de l'application consiste à intercepter les messages SMS et à lire le journal des appels. Plus de 2 200 utilisateurs ont été affectés par cet échantillon.
5. **MobileTracker.c** présente plusieurs fonctionnalités, comme l'interception de messages issus des principaux réseaux sociaux et la prise de contrôle à distance de l'appareil affecté. Plus de 2 100 utilisateurs ont été affectés par cet échantillon.
6. **PhoneSpy**, également connu sous le nom Spy Phone app ou Spapp Monitoring. Cette application comporte de nombreuses fonctionnalités d'espionnage, touchant les messageries instantanées et les réseaux sociaux les plus populaires.
7. **Agent.hb** est une autre version de MobileTracker. Comme la version originale, elle propose de nombreuses fonctionnalités.
8. **Cerberus.b**, un échantillon différent de la même famille que Cerberus.a.
9. **Reptilic.a** est un stalkerware comprenant plusieurs fonctions comme la surveillance des réseaux sociaux, l'enregistrement des appels et la surveillance de l'activité Web.
10. **SecretCam.a** est un logiciel espionnant la caméra vidéo du téléphone. Il est donc capable d'enregistrer secrètement une vidéo depuis la caméra frontale ou arrière de l'appareil affecté.

Répartition géographique des utilisateurs affectés

Les stalkerwares constituent un phénomène mondial qui affecte tous les pays, sans restriction de taille, société ou culture. En observant les 10 pays les plus affectés au monde en 2020, Kaspersky remarque que les pays affectés restent les mêmes, la Russie arrivant, de loin, en première place. Nous avons toutefois détecté une augmentation de l'utilisation des stalkerwares au Brésil et aux États-Unis en 2020 par rapport à 2019. Et les détections ont été moins nombreuses en Inde, qui descend dans le classement. Nous avons également détecté un plus grand nombre d'incidents au Mexique, qui apparaît aujourd'hui dans les premières places du classement.

	Pays	Utilisateurs affectés
1	Fédération de Russie	12 389
2	Brésil	6 523
3	États-Unis d'Amérique	4 745
4	Inde	4 627
5	Mexique	1 570
6	Allemagne	1 547
7	Iran	1 345
8	Italie	1 144
9	Royaume-Uni	1 009
10	Arabie saoudite	968

Table 4 – Top 10 des pays les plus affectés par les stalkerware en 2020 - échelle mondiale

En Europe, l'Allemagne, l'Italie et le Royaume-Uni sont respectivement les trois pays les plus affectés. Ils sont suivis par la France, en 4e position, et l'Espagne, en 5e position.

	Pays	Utilisateurs affectés
1	Allemagne	1 547
2	Italie	1 144
3	Royaume-Uni	1 009
4	France	904
5	Espagne	873
6	Pologne	444
7	Pays-Bas	321
8	Roumanie	222
9	Belgique	180
10	Autriche	153

Table 5 – Top 10 des pays les plus affectés par les stalkerwares en 2020 - Europe

Comment vérifier si un stalkerware est installé sur un appareil mobile

Il est difficile pour l'utilisateur de savoir si un stalkerware est installé sur son appareil. De façon générale, ce type de logiciel reste caché, ce qui signifie que l'icône de l'application est masquée sur l'écran d'accueil et dans le menu du téléphone. En outre, les traces de son installation ont pu être effacées. Il peut toutefois se trahir et certains signaux faibles sont à observer. Parmi eux :

- Essayez de remarquer si la batterie se décharge rapidement, si l'appareil est en surchauffe constante ou si la consommation de données mobiles est en hausse.
- Lancez régulièrement une analyse antivirus sur votre appareil Android : Si la solution de cybersécurité détecte un stalkerware, **ne le supprimez pas immédiatement, car l'agresseur qui l'a installé pourrait en être informé**. Suivez les consignes de sécurité et demandez de l'aide à une organisation locale.
- Vérifiez l'historique de votre navigateur : Pour télécharger le stalkerware, l'agresseur devra accéder à certaines pages Web dont l'utilisateur affecté n'est pas au courant. Mais l'historique peut être vide si l'assaillant l'a effacé.
- Vérifiez les paramètres relatifs aux « sources inconnues ». Si les « sources inconnues » sont activées sur votre appareil, cela peut indiquer que des logiciels indésirables ont été installés auprès d'une source tierce.
- Vérifiez les autorisations des applications installées : Les stalkerwares peuvent être masqués sous un nom factice avec un accès suspect aux messages, au journal d'appels, aux emplacements et à d'autres activités confidentielles.

Notez toutefois que ces signaux d'avertissement ne sont pas nécessairement la preuve qu'un stalkerware a été installé sur l'appareil.

Dans le contexte de violences conjugales et de relations abusives, il peut être difficile ou impossible de refuser l'accès au téléphone au conjoint.

Comment minimiser le risque ?

Certains conseils peuvent vous aider à renforcer votre sécurité numérique :

- Ne prêtez votre téléphone à personne sans voir l'usage qu'il en est fait, et ne le laissez jamais déverrouillé.*
- Utilisez un mot de passe complexe de verrouillage d'écran et modifiez vos mots de passe régulièrement.
- Ne communiquez à personne votre mot de passe, même à votre conjoint, un membre de votre famille ou à des amis.*
- Vérifiez régulièrement votre téléphone— supprimez les applications que vous n'utilisez pas et vérifiez les autorisations accordées à chacune des applications.
- Sur les appareils Android, désactivez l'option permettant l'installation d'applications tierces.
- Protégez vos appareils Android avec une solution de cybersécurité comme Kaspersky Internet Security for Android (gratuit), qui détecte les stalkerwares et vous alerte de leur présence.

*Dans le contexte de violences conjugales et de relations abusives, il peut être difficile ou impossible de refuser l'accès au téléphone au conjoint.

Activités et contribution de Kaspersky pour mettre fin à la cyberviolence

Kaspersky travaille activement pour mettre fin aux cyberviolences et à l'utilisation des stalkerwares. Elle le fait en qualité propre de société, mais aussi en collaboration avec d'autres partenaires. En 2019, nous avons développé une alerte spécifique qui avertit les utilisateurs de Kaspersky Internet Security pour Android lorsqu'un stalkerware est installé sur leur téléphone. Au cours de la même année, nous avons créé la Coalition contre les stalkerwares aux côtés de neuf autres membres fondateurs. En 2020, nous avons créé TinyCheck, un outil gratuit et open source pour détecter les stalkerwares sur appareils mobiles, en particulier à l'attention des organisations travaillant auprès des victimes de violences conjugales. Vous pouvez télécharger TinyCheck ici : https://github.com/KasperskyLab/TinyCheck. Depuis 2021, nous sommes l'un des cinq partenaires du projet européen DeStalk visant à contrer la cyberviolence et les stalkerwares , que la Commission européenne a choisi de soutenir dans le cadre de son programme Rights, Equality and Citizenship (REC).

À propos de la Coalition contre les stalkerwares

La Coalition contre les stalkerware (« CAS » ou « Coalition ») est un groupe qui se consacre aux violences et au harcèlement générés par l'utilisation des stalkerwares. Lancée en novembre 2019, la Coalition contre les stalkerwares a réuni 26 partenaires dès sa première année. Parmi ces partenaires fondateurs : 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 et WEISSER RING. La Coalition vise à rassembler des organisations de divers horizons pour lutter activement contre le comportement criminel permis par les stalkerwares et œuvre à la sensibilisation des publics face à ce phénomène majeur. Du fait du fort impact pour les utilisateurs du monde entier, mais aussi des nouvelles variantes de stalkerwares apparaissant régulièrement, la Coalition contre les stalkerwares est ouverte à tous les nouveaux partenaires et appelle à une coopération élargie. Pour en savoir plus sur Coalition contre les stalkerwares, visitez le site https://stopstalkerware.org/fr.