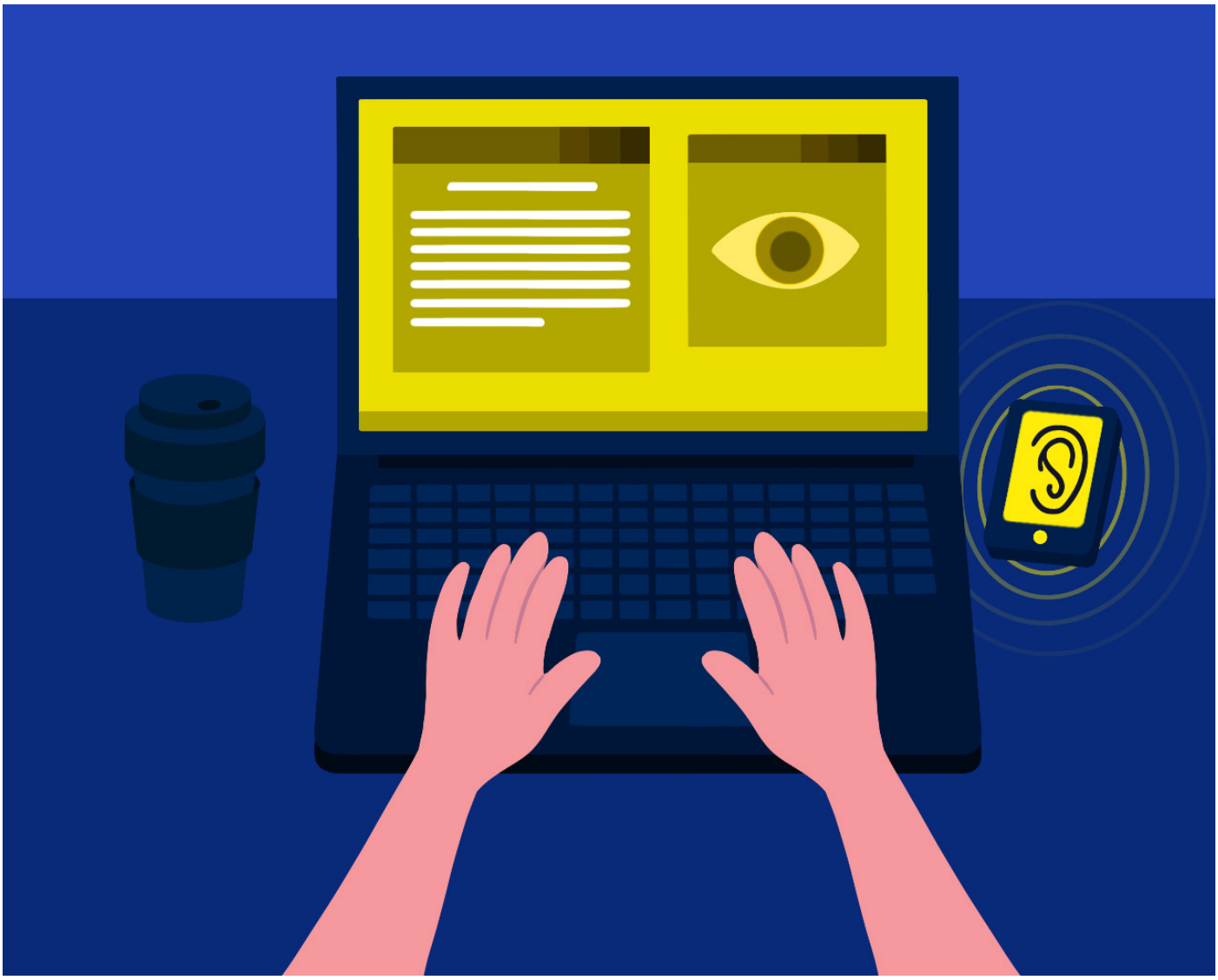


Le point sur les **stalkerwares** en 2021

COALITION AGAINST STALKERWARE

kaspersky

Contenu

Principaux enseignements de l'année 2021

Tendances observées par Kaspersky

L'utilisation des stalkerwares est en baisse, mais la violence, quant à elle, est en hausse

Comment Kaspersky et ses partenaires collaborent pour lutter contre les stalkerwares

L'année 2021 a été le théâtre d›avancées positives sur les plans réglementaire et institutionnel

Vous pensez être suivi(e) par un stalkerware ? Voici quelques conseils

Principaux enseignements de l'année 2021

Kaspersky analyse chaque année l'utilisation des stalkerwares dans le monde pour mieux comprendre la menace qu'ils représentent. Nous travaillons en partenariat avec des acteurs des secteurs privé et public pour sensibiliser les utilisateurs et trouver des solutions afin de lutter contre ce problème majeur.

Les stalkerwares permettent d'espionner secrètement la vie privée des individus via leurs appareils numériques et sont souvent utilisés comme levier de violence psychologique et physique dans le cadre des relations intimes. Disponibles dans le commerce, les logiciels ont accès à une multitude de données personnelles, notamment la localisation de l'appareil, l'historique du navigateur, les SMS, les discussions sur les réseaux sociaux, les photos, et bien plus encore. La commercialisation des stalkerwares est légale, son utilisation sans le consentement de la victime en revanche, ne l'est pas. Les auteurs de ces actes profitent du cadre juridique vague qui existe encore dans de nombreux pays. Les stalkerwares constituent une violation de la vie privée et une forme d'abus technologique. Pour lutter contre cette menace complexe de manière globale, et qui soutienne au mieux les victimes et les rescapés, des outils innovants sur les plans législatif, social et technologique sont nécessaires.

Messages et données clés de l'année 2021

- **Selon les données de Kaspersky, 32 694 utilisateurs uniques ont été affectés par des stalkerwares dans le monde en 2021.** Ce chiffre est inférieur aux chiffres enregistrés en 2020 et constitue une baisse historique depuis le début de notre collecte de données sur les stalkerwares en 2018. Devrions-nous nous en réjouir ? La réponse est non.
- **La cyberviolence est en hausse,** surtout depuis le début de la pandémie. Les gens ayant continué à moins socialiser et à passer plus de temps chez eux en 2021, les agresseurs se sont sentis plus en contrôle, et donc ils ont peut-être été moins enclins à installer des stalkerwares sur le téléphone de leurs partenaires pour les espionner. En outre, ils disposent malheureusement d'une kyrielle de moyens d'espionner ou de traquer leurs victimes via les appareils intelligents. Les ONG avec lesquelles Kaspersky travaille en étroite collaboration ont partagé les mêmes observations sur les agresseurs et les victimes de stalkerwares. Notons également que ces chiffres incluent uniquement les utilisateurs Kaspersky : ils n'englobent pas les utilisateurs de solutions de sécurité informatique concurrentes, ni ceux qui n'ont aucune solution de sécurité informatique installée sur leurs appareils mobiles. En conséquence, ce que nous voyons n'est que la partie visible de l'iceberg : même s'il est difficile de calculer le nombre exact d'utilisateurs concernés dans le monde, la Coalition contre les Stalkerware (Coalition Against Stalkerware) estime qu'il pourrait être 30 fois supérieur, avoisinant le million de victimes à l'échelle internationale, et ce, chaque année.

- Selon les données collectées par Kaspersky Security Network, **les pays les plus affectés demeurent la Russie, le Brésil et les États-Unis.** Ceci est en ligne avec les statistiques des deux dernières années. Sur le plan régional, nous enregistrons les chiffres les plus élevés d'utilisateurs affectés dans les pays suivants :
  - Allemagne, Italie et Royaume-Uni (Europe)
  - Turquie, Égypte et Arabie saoudite (Moyen-Orient et Afrique)
  - Inde, Indonésie et Vietnam (Asie-Pacifique)
  - Brésil, Mexique et Colombie (Amérique latine)
  - États-Unis (Amérique du Nord)
  - Fédération de Russie, Ukraine et Kazakhstan (Europe de l'Est (hors pays de l'UE), Russie et Asie centrale)
- **Les applications de stalkerware Cerberus et Reptilicus ont été les plus utilisées**, avec respectivement 5 575 et 4 417 utilisateurs affectés dans le monde.

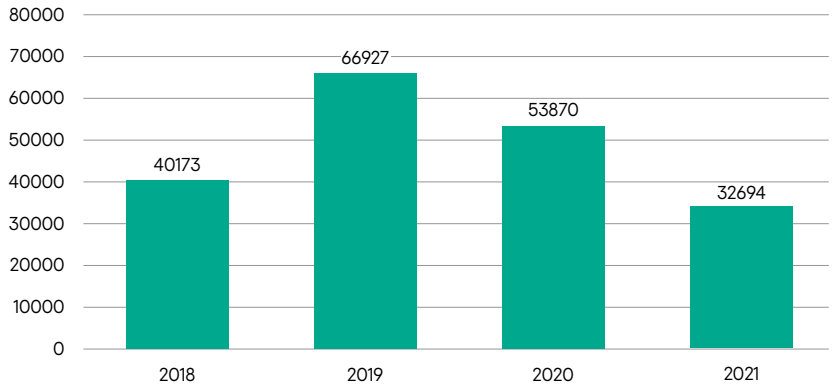
Tendances observées par Kaspersky

Chiffres des détections à l'échelle mondiale : utilisateurs affectés

Dans cette section, nous mettons l'accent sur les chiffres mondiaux et régionaux enregistrés par Kaspersky en 2021 et les comparons avec ceux des années précédentes.

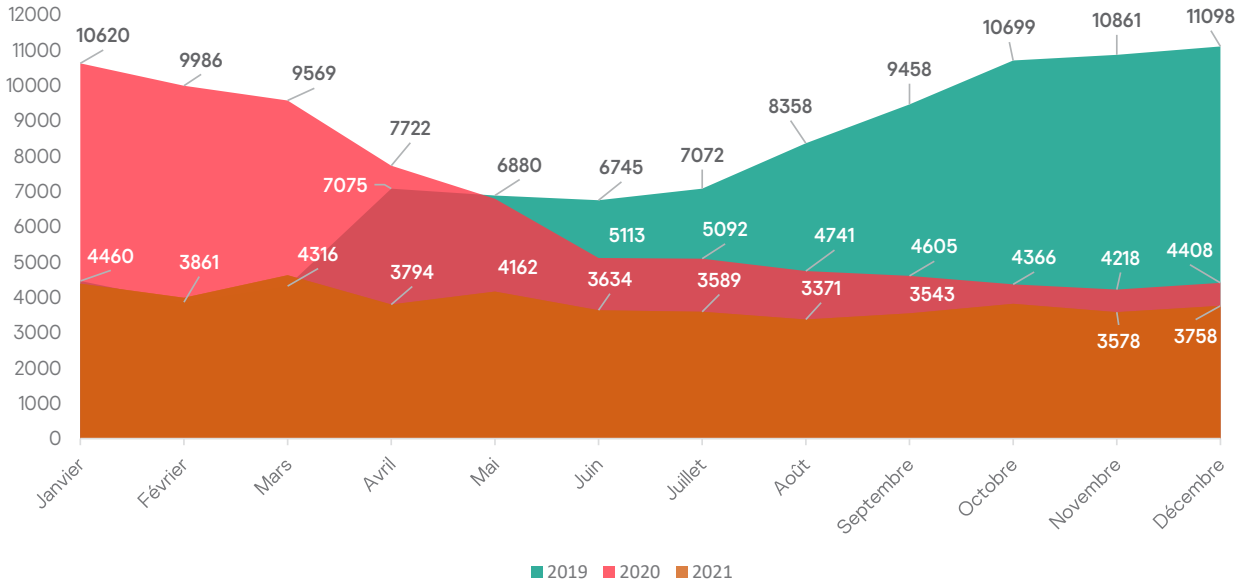
En 2021, 32 694 utilisateurs uniques ont été affectés par des stalkerwares

En 2021, 32 694 utilisateurs uniques ont été affectés par des stalkerwares. Le graphique ci-dessous illustre l'évolution des utilisateurs affectés année après année depuis 2018.



L'évolution des utilisateurs affectés année après année depuis 2018

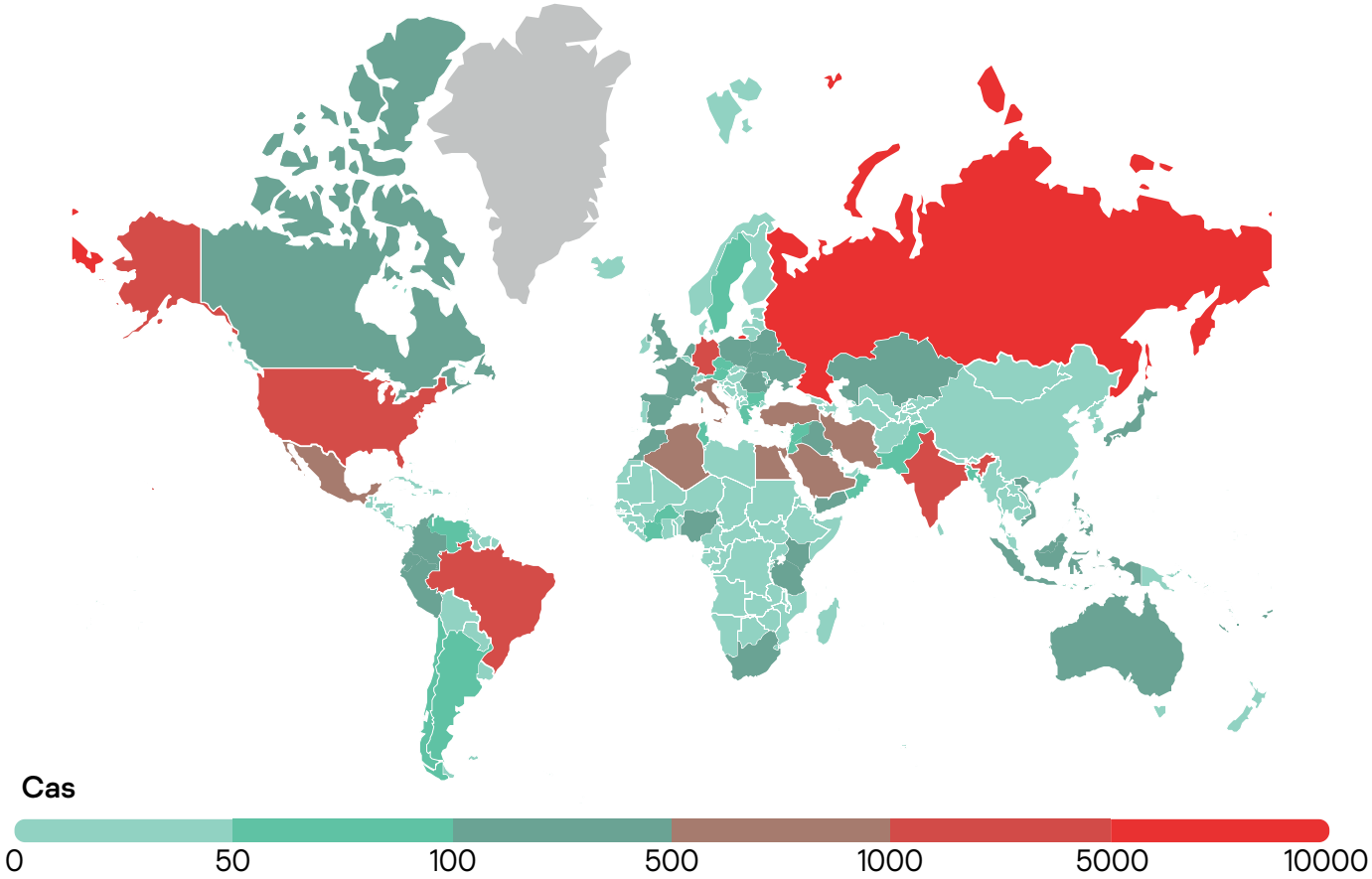
Le graphique ci-dessous montre les utilisateurs affectés par mois sur la période 2019-2021. Nous constatons que la tendance était plus stable en 2021 qu'en 2020, avec une baisse visible pendant les mois les plus impactés par les confinements et les mesures de quarantaine.



Utilisateurs uniques affectés par mois sur la période 2019-2021

Chiffres des détections à l'échelle mondiale et régionale : géographie des utilisateurs affectés

Les stalkerwares ont continué à cibler les utilisateurs du monde entier en 2021 : Kaspersky a détecté des utilisateurs affectés dans 185 pays ou territoires.



Méthodologie

Les données de ce rapport proviennent des statistiques agrégées sur les menaces obtenues par Kaspersky Security Network. Kaspersky Security Network est dédié au traitement des flux de données de cybersécurité provenant de millions de participants volontaires aux quatre coins du monde. L'ensemble des données reçues sont anonymes. Pour calculer nos statistiques, nous étudions la ligne dédiée aux utilisateurs de solutions de sécurité mobile Kaspersky en appliquant uniquement le critère de détection et la définition de la Coalition contre les stalkerware. Cela signifie que les utilisateurs affectés ont été ciblés uniquement par un stalkerware. D'autres types d'applications de surveillance ou de spywares ne s'inscrivant pas dans la définition de la Coalition sont exclues de nos statistiques.

Les statistiques reflètent les utilisateurs uniques d'appareils mobiles affectés par des stalkerwares, un chiffre qui diffère du nombre de détections. Ce dernier risque d'être supérieur puisque nous pouvons détecter un stalkerware plusieurs fois sur l'appareil d'un même utilisateur, si celui-ci décide de ne pas supprimer l'application après avoir reçu notre notification.

Enfin, ces statistiques reflètent uniquement les utilisateurs d'appareils mobiles qui utilisent des solutions de sécurité informatique Kaspersky. Certains utilisateurs peuvent installer une autre solution de cybersécurité sur leurs appareils, quand d'autres n'en utilisent aucune.

Comme en 2020, la Russie, le Brésil, les États-Unis et l'Inde sont à nouveau les quatre pays comptant le plus d'utilisateurs affectés identifiés. Le Mexique est passé de la 5e à la 9e place, et l'Algérie, la Turquie et l'Égypte ont fait leur entrée dans le top 10. Ces pays ont remplacé l'Italie, le Royaume-Uni et l'Arabie saoudite, qui ne font plus partie des 10 premiers pays les plus affectés par les stalkerwares.

	Pays	Utilisateurs affectés
1	Russie	7541
2	Brésil	4807
3	États-Unis	2319
4	Inde	2105
5	Allemagne	1012
6	Iran (République islamique d')	891
7	Algérie	665
8	Turquie	660
9	Mexique	657
10	Égypte	640

Tableau 1 : Les 10 premiers pays au monde affectés par des stalkerwares en 2021

Ce rapport fournit des statistiques régionales plus détaillées avec des chiffres pour l'Europe, la zone Asie-Pacifique, l'Amérique latine, l'Amérique du Nord, l'Europe de l'Est (hors pays de l'UE) ainsi que les zones Russie et Asie centrale, et Moyen-Orient et Afrique.

En Europe, le nombre total d'utilisateurs affectés s'élevait à 4 236 en 2021. L'Allemagne, l'Italie et le Royaume-Uni figurent en tête de liste, conservant un classement similaire à celui de l'année précédente. L'Autriche a quant à elle été remplacée dans le top 10 par la République tchèque.

	Pays	Utilisateurs affectés
1	Allemagne	1012
2	Italie	611
3	Royaume-Uni et Irlande du Nord	430
4	France	410
5	Pologne	321
6	Espagne	321
7	Pays-Bas	165
8	Roumanie	125
9	Belgique	94
10	République tchèque	82

Tableau 2 : Les 10 premiers pays d'Europe affectés par des stalkerwares en 2021

En Europe de l'Est (hors pays de l'UE), en Russie et en Asie centrale, le nombre total d'utilisateurs affectés s'élevait à 9 207. Les trois premiers pays étaient la Russie, l'Ukraine et le Kazakhstan.

	Pays	Utilisateurs affectés
1	Russie	7541
2	Ukraine	490
3	Kazakhstan	461
4	Biélorussie	250
5	Ouzbékistan	223
6	Azerbaïdjan	92
7	République de Moldavie	51
8	Tadjikistan	49
9	Kirghizistan	40
10	Turkménistan	19

Tableau 3 : Les 10 premiers pays d'Europe de l'Est (hors pays de l'UE), de Russie et d'Asie centrale touchés par des stalkerwares en 2021

Au Moyen-Orient et en Afrique, le nombre total d'utilisateurs affectés s'élevait à 6 270, la Turquie, l'Égypte et l'Arabie saoudite enregistrant les chiffres les plus élevés.

	Pays	Utilisateurs affectés
1	Turquie	660
2	Égypte	640
3	Arabie saoudite	575
4	Kenya	271
5	Afrique du Sud	240
6	Émirats arabes unis	143
7	Nigeria	123
8	Koweït	68
9	Oman	58
10	Éthiopie	46

Tableau 4 : Les 10 premiers pays de la zone Moyen Orient et Afrique affectés par des stalkerwares en 2021

Dans la zone Asie-Pacifique, le nombre total d'utilisateurs affectés s'élevait à 4 243. L'Inde se positionnait bien au-dessus des autres pays avec 2 105 utilisateurs affectés, suivie par l'Indonésie et le Vietnam.

	Pays	Utilisateurs affectés
1	Inde	2105
2	Indonésie	353
3	Vietnam	258
4	Philippines	240
5	Malaisie	229
6	Australie	205
7	Bangladesh	169
8	Japon	167
9	Pakistan	98
10	Sri Lanka	83

Tableau 5 : Les 10 premiers pays de la zone Asie-Pacifique affectés par des stalkerwares en 2021

Le classement de l'Amérique latine et de la région des Caraïbes était dominé par le Brésil, représentant 72,5 % du nombre total d'utilisateurs affectés dans la région (alors que le pays ne représente qu'environ 32 % de la population régionale). Venaient ensuite le Mexique et la Colombie. On a enregistré 6 609 utilisateurs affectés dans toute la région.

	Pays	Utilisateurs affectés
1	Brésil	4807
2	Mexique	657
3	Colombie	202
4	Équateur	192
5	Pérou	179
6	Argentine	90
7	Chili	73
8	Venezuela	58
9	Bolivie	46
10	Haïti	36

Tableau 6 : Les 10 premiers pays d'Amérique latine et Caraïbes affectés par des stalkerwares en 2021

Enfin, en Amérique du Nord, les États-Unis représentaient 87 % de l'ensemble des utilisateurs affectés dans la région, un chiffre prévisible puisque la population y est dix fois supérieure à celle du Canada. Le nombre total d'utilisateurs affectés en Amérique du Nord, sans compter le Mexique qui a été inclus dans les données d'Amérique latine, s'élève à 2 666.

	Pays	Utilisateurs affectés
1	États-Unis	2319
2	Canada	347

Tableau 7 : Utilisateurs affectés par des stalkerwares en 2021 – Amérique du Nord

Fonctionnalités courantes des applications de stalkerware

Cette section répertorie les applications de stalkerware les plus utilisées pour contrôler les appareils mobiles à l'échelle mondiale. Les applications de stalkerware Cerberus et Reptilicus ont été les plus utilisées, avec respectivement 5 575 et 4 417 utilisateurs affectés dans le monde.

	Nom de l'application	Utilisateurs affectés
1	Cerberus	5,575
2	Reptilicus (ou 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

Tableau 8 : Les principales applications de stalkerware de l'année 2021

Les applications de stalkerware peuvent donner à leurs utilisateurs un pouvoir immense et un accès total au téléphone mobile de leur victime, selon leurs caractéristiques et leur utilisation gratuite ou payante. Certaines sont commercialisées en tant qu'applications antivol ou de contrôle parental, mais elles sont en réalité très différentes à de multiples égards, à commencer par le fait qu'elles opèrent discrètement, à l'insu de la victime et sans son consentement.

La plupart des applications populaires fournissent les fonctionnalités de stalkerware courantes. Par exemple :

- Icône permettant de masquer l'application
- Lecture des SMS, MMS et journaux d'appels
- Accès aux listes de contacts

Les systèmes d'exploitation Android et iOS sont-ils affectés de la même façon par les stalkerwares ?

Les outils de stalkerware sont moins fréquents sur les iPhones que sur les appareils Android car le système d'exploitation iOS est traditionnellement fermé. Les agresseurs peuvent contourner cette restriction sur des iPhones débridés, mais ils auront néanmoins toujours besoin d'un accès physique aux téléphones pour cette manipulation. Les utilisateurs d'iPhones qui craignent une surveillance doivent dans la mesure du possible, toujours garder un œil sur leur appareil.

Un agresseur peut également offrir un iPhone ou tout autre appareil à sa victime avec un stalkerware préinstallé. Les entreprises proposant ce service en ligne sont nombreuses et permettent aux agresseurs d'installer ces outils sur de nouveaux téléphones, qui peuvent ensuite être livrés à la victime dans un emballage d'usine sous couvert de cadeau.

- Localisation GPS
- Suivi des événements du calendrier
- Lecture des messages émanant des services de messagerie et des réseaux sociaux populaires comme 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, etc.
- Affichage des photos des galeries des téléphones
- Prise de captures d'écran
- Prise de portraits avec l'appareil photo

L'utilisation des stalkerwares est en baisse, mais la violence, quant à elle, est en hausse

Le nombre d'utilisateurs affectés et certains comportements et perceptions par rapport à l'utilisation des stalkerwares demeurent préoccupants

Même si nous enregistrons une baisse de 39 % d'utilisateurs affectés par rapport à nos données de 2020, la lutte contre les stalkerwares et la cyberviolence est loin d'être terminée. Le nombre d'utilisateurs affectés et certains comportements et perceptions par rapport à l'utilisation des stalkerwares demeurent préoccupants. En novembre dernier, Kaspersky a commandité une enquête mondiale impliquant plus de 21 000 participants dans 21 pays sur leurs attitudes vis-à-vis de la vie privée et du harcèlement numérique dans le cadre des relations intimes. Même si la majorité des participants (70 %) estime inacceptable le fait de surveiller son partenaire sans son consentement, un nombre significatif (30 %) d'entre eux n'y voient pas un problème et justifient un tel comportement dans certaines circonstances. Parmi les personnes estimant qu'une surveillance secrète peut être justifiée, presque deux tiers envisageraient d'utiliser de telles applications en cas de doute sur la fidélité de leur partenaire (64 %) ou d'insécurité (63 %), et la moitié l'envisageraient également s'ils pensaient que leur partenaire était impliqué dans des activités criminelles (50 %).

Les TIC sont de puissants outils pour les agresseurs exerçant un contrôle coercitif, notamment dans le cadre des relations intimes où la violence est déjà présente hors ligne

L'Internet à haut débit, combiné à la propagation rapide des technologies de l'information et de la communication (TIC) ont contribué à cette cyberviolence en créant de nouveaux outil permettant aux agresseurs de partager des contenus violents et dangereux ou d'adopter des comportements causant des dommages affectifs, psychologiques ou physiques chez les victimes. Alors même que ces technologies ont donné aux gens la possibilité de conserver des relations sociales et affectives malgré la distance physique, les TIC ont également été un vecteur de cyberviolence, une conséquence dont les profondes répercussions s'étendent au monde hors ligne avec de réels impacts négatifs sur les victimes.

Les résultats de notre étude corroborent ces constats : 15 % de participants à l'échelle mondiale ont déclaré avoir déjà été contraints par leur partenaire d'installer une application de surveillance. 34 % des participants ayant donné cette réponse ont également confirmé être la cible d'agressions physiques et/ou verbales.

Même s'il est trop tôt pour tirer des conclusions définitives sur la baisse des utilisateurs affectés en 2021, deux théories peuvent expliquer cette tendance.

Tout d'abord, nous pensons que l'ensemble des aspects de nos vies ont toujours fortement été impactés par la pandémie en 2021. Des études récentes ont démontré que de nouveaux comportements ont fait surface dans des domaines aussi variés que le travail, l'apprentissage, le foyer, la consommation, les communications et l'information, les voyages et la mobilité. Pour résumer, les gens sont restés davantage chez eux (49 % évitaient de quitter leur domicile et 50 % travaillaient chez eux, partiellement ou à temps plein), réduisant les interactions en face-à-face (57 % indiquaient qu'ils prenaient leurs distance avec leurs amis et leur communauté) et les voyages, alors que les achats, les formations et les divertissements en ligne n'ont cessé de croître. Ainsi, les agresseurs auraient eu moins besoin de surveiller leur partenaire, qui se trouvait désormais la plupart du temps avec eux.

D'autre part, l'Internet des objets (IoT, Internet of Things) et la digitalisation sont aujourd'hui omniprésents dans nos vies. Ils envahissent nos routines, nos foyers, nos voitures et nos bureaux. Même si les opportunités et les avantage des objets connectés sont infinis, de nombreux appareils permettent également à des tiers de nous espionner. Selon notre étude, les agresseurs ont ainsi utilisé d'autres moyens que les stalkerwares pour espionner leur partenaire : 50 % des participants indiquent qu'ils ont été suivis via des applications sur mobile, 29 % mentionnent qu'ils ont été surveillés par le biais de dispositifs de géolocalisation, 22 % par des webcams et 18 % par des appareils de la maison connectée.

La publication d'Apple en janvier 2022 d'un manuel de sécurité pour son produit AirTag marque un tournant dans notre perception de la situation.

Les organisations NNEDV (National Network to End Domestic Violence) et WWP EN (European Network for the Work with Perpetrators of Domestic Violence) partagent avec nous leur expérience et leur point de vue sur ces deux théories et sur l'abus numérique en général.

WWP EN

Le réseau WWP EN est une association d'organisations travaillant directement ou indirectement avec des personnes perpétrant des violences dans le cadre des relations intimes. Il est spécialisé dans la violence perpétrée par les hommes contre les femmes et les enfants. Sa mission consiste à renforcer la sécurité des femmes et des enfants, ainsi que des autres personnes menacées dans le cadre de leurs relations intimes grâce à un travail efficace auprès des auteurs de ces violences, principalement des hommes.

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

Comment les mesures imposées par les gouvernements pendant la pandémie ont facilité et renforcé le contrôle coercitif des agresseurs — Berta Vall Castelló, Responsable Recherche & Développement et Anna McKenzie, Responsable Communications pour le réseau WWP EN

Le contrôle coercitif se définit comme « un schéma de comportements abusifs destinés à exercer une domination et un contrôle sur l'autre partie dans une relation. Il peut englober différents comportements abusifs, qu'ils soient physiques, psychologiques, affectifs ou financiers, qui, en s'accumulant, privent au fil du temps les victimes/rescapés de leur autonomie et de leur indépendance en tant qu'individu » (McGorrery et McMahon, 2020). Comme nous l'écrivons dans notre manuel « Same Violence, New Tools – How to work with violent men who use cyberviolence » (Une même violence, de nouveaux outils – Comment travailler avec les hommes violents qui utilisent la cyberviolence), les auteurs d'abus isolent leur partenaire, qui devient alors dépendant sur le plan affectif. Ils ont recours aux agressions, aux menaces, à l'intimidation, à l'humiliation, à l'isolement et à bien d'autres moyens pour instaurer un climat permanent de crainte, ainsi qu'une perte générale du sentiment de liberté. Les TIC sont de puissants outils pour les agresseurs exerçant un contrôle coercitif, notamment dans le cadre des relations intimes où la violence est déjà présente hors ligne.

Une étude récente sur les violences domestiques pendant la pandémie de COVID-19 a révélé que les mesures imposées par les gouvernements pendant le confinement avaient facilité le contrôle coercitif des auteurs d'abus. Les auteurs suggèrent que les mesures d'isolement/de distanciation physique ont empiété sur les stratégies de contrôle coercitif adoptées par les agresseurs pour contrôler leur partenaire (Pentaraki et Speake, 2020). Compte tenu de ces conclusions, il est probable que les agresseurs ressentent moins le « besoin » d'utiliser des stalkerwares pour exercer un contrôle coercitif sur leur partenaire. Par ailleurs, une récente étude a observé que les abus informatisés augmentaient souvent pendant une période de séparation (George et Harris 2014 ; Woodlock 2016). Ainsi, pendant une situation de confinement avec des couples contraints de rester à la maison, le recours aux abus informatisés est moins utile.

Les mesures imposées par les gouvernements pendant le confinement avaient facilité le contrôle coercitif des auteurs d'abus

Rappelons-nous qu'une baisse de l'utilisation des stalkerwares n'équivaut pas à une baisse de la violence conjugale pendant la pandémie. Bien au contraire, Boxall, Morgan et Brown (2020) notent que la violence conjugale a augmenté pendant la pandémie de COVID-19. C'est ainsi que rapport indique que les stalkerwares ont été remplacés par d'autres outils. Elena Gajotto, travaillant pour l'ONG Una Casa per l'Uomo, remarque : « Il est si facile de surveiller et de suivre quelqu'un par exemple en utilisant son compte Google, qu'on n'a pas vraiment besoin d'utiliser de stalkerware. » La multitude d'abus numériques peut avoir eu un impact sur la baisse de l'utilisation des stalkerwares en particulier. Letizia Baroncelli, qui travaille pour l'ONG Centro Ascolto Uomini Malttratanti (CAM), acquiesce et ajoute : « Je pense que nous voyons moins de stalkerwares parce qu'il existe de nombreuses autres façons de perpétrer des abus numériques. »

Les ONG, les gouvernements et les chercheurs ont enregistré une hausse significative des abus utilisant images et sextorsions depuis le début de la pandémie (Boniello, 2020 ; CCRI, Communication personnelle, 2 juin 2020 ; FBI, 2020, 2021). Il semble que ce type d'abus numérique a augmenté, particulièrement parmi les adolescents et les couples qui ne vivent pas ensemble. Letizia Baroncelli poursuit : « Le partage des images personnelles a fortement augmenté depuis la pandémie, notamment parmi les jeunes agresseurs, qui n'ont pas conscience de commettre un crime. » Elena Gajotto rajoute : « L'abus par le biais d'images est dévastateur chez les femmes, alors que les hommes ne comprennent même pas qu'ils ont fait quelque chose de mal. »

Selon plusieurs membres du réseau WWP EN, la forme de violence numérique la plus courante est la surveillance par les hommes des activités numériques de leur partenaire, comme les emails, les téléphones et les comptes de réseaux sociaux. Ceci vient conforter les observations de Daniel Antunovic, travaillant pour l'ONG croate NGO UZOR, qui convient que les formes « primitives » de suivi numérique sont les plus fréquentes.

Le WWP EN oriente son travail sur les abus numériques pour garantir la sécurité des victimes. Elena Gajotto continue : « Près de la moitié des hommes partagent leurs actes de violence numérique sans réaliser qu'il s'agit d'abus. Si nous ne nous focalisons pas explicitement sur ce type de violence dans notre travail avec les agresseurs, rien ne changera. » Il est donc nécessaire d'aider les professionnels

qui travaillent auprès des agresseurs et des victimes de violence domestique pour dépister les cas de violence numérique et intervenir. Daniel Antunovic explique : « Nous n'avons pas enregistré autant de cas de violence numérique que je l'imaginais depuis la pandémie de COVID-19. Néanmoins, les abus numériques s'apparentent en quelque sorte à de la violence sexualisée. Cela arrive souvent, mais reste caché. »

Il y a de plus en plus « d'appareils intelligents » utilisés pour perpétrer des violences conjugales — Toby Shulruff, Responsable du project Tech Safety pour le réseau NNEDV

Même si les stalkerwares sont un problème fréquent, il existe de nombreux autres outils à la disposition des agresseurs qui ressemblent à des stalkerwares, mais qui n'en sont pas. Par exemple, les informations personnelles disponibles en ligne et les fonctionnalités quotidiennes des appareils et des comptes peuvent être utilisées pour localiser une personne ou suivre son activité. La complexité et les connexions entre les appareils, les comptes et les informations sur Internet n'aident pas les victimes et ceux qui travaillent avec elles à évaluer la situation et à réagir efficacement. Il peut être terrifiant et insurmontable pour un rescapé de prendre conscience qu'un agresseur connaît de multiples détails sur son quotidien.

Malheureusement, de plus en plus d'appareils « intelligents », comme les assistants domestiques, les appareils électroménagers connectés, les systèmes de sécurité connectés aux réseaux wifi et les smartphones, sont utilisés pour perpétrer des actes de violence conjugale.

Selon une étude réalisée par le réseau NNEDV en décembre 2020 et janvier 2021, chaque type d'abus numérique a augmenté pendant la pandémie. Même si on sait que les téléphones représentent la technologie la plus utilisée de façon inappropriée (dans 87 % des cas selon l'étude), les appareils « intelligents » ou connectés sont également identifiés comme de plus en plus utilisés dans le contexte de l'abus numérique. Près d'un tiers des professionnels travaillant auprès de victimes le confirme.

NNEDV

Le projet Safety Net du réseau NNEDV met l'accent sur le croisement entre technologie, vie privée, confidentialité et innovation, des notions qui ont toutes un lien avec la sécurité et les violences. Le projet préconise de mettre en place des politiques pour mieux soutenir les victimes, de former les professionnels dans le système judiciaire et de davantage collaborer avec les communautés, et les sociétés du numérique afin de lutter contre la violence numérique, soutenir les rescapés dans leur utilisation de la technologie et d'exploiter celle-ci pour améliorer les services.

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

De plus en plus d'appareils « intelligents », comme les assistants domestiques, les appareils électroménagers connectés, les systèmes de sécurité connectés aux réseaux wifi et les smartphones, sont utilisés pour perpétrer des actes de violence conjugale

De plus en plus de personnes adoptant des appareils IoT, ce phénomène ne va cesser de croître. Ces produits sont prévus pour plus de confort et d'efficacité. La fabrication d'appareils IoT est un marché qui émerge rapidement avec à la fois des acteurs majeurs et bien établis et de nombreuses nouvelles entreprises plus petites[1]. L'IoT est possible grâce à plusieurs tendances technologiques qui s'entrecroisent : la miniaturisation, la capacité accrue de traitement d'information, le stockage de davantage de données, le coût de fabrication moindre et la connectivité.

En raison de plusieurs facteurs tels que la pression des marchés, l'émergence rapide de la technologie et la complexité de l'IoT, des risques majeurs de sécurité et de confidentialité sont de plus en plus visibles[2]. Les appareils domestiques connectés, en particulier, sont aujourd'hui utilisés dans un contexte de violence conjugale pour contrôler et menacer les victimes. [Les chercheurs du projet Gender + IoT à l'University College de Londres[3] ont exploré les dommages faits aux victimes] [et proposent des solutions en partenariat avec les professionnels d'aide aux victimes sur le terrain.]

La récente étude du NNEDV a documenté la multiplication d'abus numériques pendant la pandémie. Nous sommes préoccupés parce qu'alors que nous sortons de cette crise sanitaire publique, les auteurs d'abus qui ont adopté ces tactiques ou augmenté leurs abus numériques pendant cette période, ne seront nullement incités à changer de comportement. Une récente étude[4] suggère que les professionnels d'aide aux victimes devraient se focaliser sur tous les types d'abus numériques, notamment les stalkerwares et les appareils domestiques connectés. Il est fort probable que le pic d'abus numériques constaté par les professionnels perdure. Nous devons impérativement continuer à soutenir les victimes et travailler à la prévention des abus numériques.

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., et Danezis, G. (2018). The rise of the Internet of Things and implications for technology-facilitated abuse (L'expansion de l'Internet des objets et les conséquences pour les abus informatisés). University College de Londres.

4 Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. et Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders (Les technologies numériques et la violence conjugale : analyse qualitative avec de nombreuses parties prenantes). Proceedings of the ACM on human-computer interaction (Compte rendu de l'ACM sur l›interaction humain/machine), 1(CSCW), p.1-22.

Comment Kaspersky et ses partenaires collaborent pour lutter contre les stalkerwares

Le sujet des stalkerwares n'est pas un simple problème technique : toutes les sphères de la société doivent s'impliquer pour s'atteler à ce fléau. Depuis quelques années, Kaspersky est au premier plan des débats sur le sujet. Nous sensibilisons les acteurs privés et publics pour qu'ils comprennent mieux le problème et trouvent des solutions communes. Nous contribuons au développement de formation et d'outils pratiques pour aider les organisations à but non lucratif, les institutions et les individus à renforcer leur résilience face aux stalkerwares. Nous organisons et participons à des webinaires et des tables rondes avec des institutions pour échanger et contribuer aux discussions qui façonneront la législation de demain.

Kaspersky est l'un des cofondateurs et un pilier de la Coalition contre les stalkerware (Coalition Against Stalkerware), un groupe de travail international dédié à la lutte contre les stalkerwares et la violence domestique. La coalition réunit des organisations qui travaillent avec des victimes et des auteurs d'abus, des activistes numériques et des fournisseurs de solutions de cybersécurité. Cette plateforme unique permet à l'ensemble des parties prenantes concernées de partager leurs meilleures pratiques et de réunir leurs efforts pour combattre les stalkerwares.

Kaspersky est également l'un des partenaires du projet DeStalk. Financé par la Commission européenne, ce projet de recherche vise à élaborer une stratégie pour former et soutenir entre autre, les professionnels travaillant dans les services d'aide aux victimes et les programmes destinés aux agresseurs, les institutions ou les gouvernements locaux. Le consortium prévoit de mettre à niveau et de tester les outils existants pour les praticiens et développe une campagne de sensibilisation pilote régionale en Italie.

En 2021, nous avons collaboré avec INTERPOL et deux organisations à but non lucratif américaine et australienne pour proposer deux sessions de formation en ligne aux agents des forces de l'ordre. Ces sessions ont été suivies par plus de 210 participants venant du monde entier.

Fin 2021, Kaspersky a également participé à l'événement « Combating violence against women in a digital age - utilising the Istanbul Convention » (Combattre la violence contre les femmes à l'ère du numérique en s'appuyant sur la Convention d'Istanbul), organisée par le Conseil de l'Europe. Cet événement a été l'occasion de discuter des recommandations du GREVIO (Group of Experts on combating Violence against women and domestic violence, groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique).

TinyCheck : un outil pour venir en aide aux victimes de violence domestique

Le travail de Kaspersky avec l'outil TinyCheck est une initiative qu'il est important de mentionner. Il s'agit d'un outil open source gratuit, développé et soutenu par Kaspersky. Initialement créé pour aider les ONG à protéger les victimes de violence domestique et leur vie privée, TinyCheck facilite la détection des stalkerwares sur les téléphones des victimes, qu'importe le système d'exploitation, de façon simple, rapide et non invasive, sans que l'auteur de l'abus ne s'en rende compte. Même si les solutions de sécurité peuvent également vérifier et signaler la présence de stalkerwares, elles doivent être installées sur l'appareil. L'agresseur risque donc d'être alerté. Des projets tels que le développement de l'outil TinyCheck visent à garantir que les victimes puissent utiliser leurs appareils sans crainte d'être surveillés.

TinyCheck facilite la détection des stalkerwares sur les téléphones des victimes, de façon simple, rapide et non invasive, sans que l'auteur de l'abus ne s'en rende compte

Avec TinyCheck, nul besoin d'installer d'applications sur le téléphone pour effectuer une vérification. Les résultats ne s'affichent pas et ne sont pas transmises sur l'appareil potentiellement affecté. Par ailleurs, TinyCheck permet aux victimes de vérifier n'importe quel appareil, indépendamment du système d'exploitation (iOS, Android ou autre). Ces fonctionnalités relèvent deux défis majeurs liés à la protection des utilisateurs contre les stalkerwares. L'outil a été développé pour fonctionner sur un Raspberry Pi avec une connexion wifi ordinaire. TinyCheck analyse rapidement le trafic sortant d'un appareil mobile et identifie les indicateurs de compromission (Indicators of Compromise, IOC) tels que les interactions avec des sources malveillantes connues comme les serveurs associés aux stalkerwares. Aujourd'hui, l'outil utilise les IOC collectés non seulement par les chercheurs de Kaspersky, mais aussi par les référentiels conservés par des chercheurs indépendants (merci à Étienne Maynier, ou Tek, d'Echap et Cian Heasley). Nous espérons que la communauté continuera ce travail en maintenant les IOC à jour.

Cela étant dit, il faut bien comprendre que TinyCheck a certaines limites. L'outil doit être utilisé en tenant compte du point suivant : les IOC ne détectent pas complètement et en temps réel l'ensemble des applications de stalkerware comme le fait une solution de sécurité informatique. Par conséquent, un résultat ne détectant aucun stalkerware n'exclut pas la possibilité que le stalkerware soit installé, mais non détecté par TinyCheck.

En 2021, davantage d'ONG spécialisées dans la violence domestique ont testé TinyCheck et fourni leur retour d'expérience pour aider à améliorer le service. Les forces de police et les instances judiciaires de plusieurs pays ont également porté un intérêt à l'outil pour mieux soutenir les victimes.

L'année 2021 a été le théâtre d›avancées positives sur les plans réglementaire et institutionnel

À travers le monde, 2021 se distingue par des avancées positives dans la lutte contre les stalkerware d'un point de vue réglementaire et institutionnel. En mai 2021, la Diète, le parlement japonais, a promulgué un projet de loi pour amender sa réglementation sur les stalkerwares. Selon la nouvelle loi, en plus des autres clauses, l'obtention d'informations de localisation des smartphones d'individus grâce à des applications sans leur autorisation est désormais illégale.

En août 2021, la Federal Trade Commission des États-Unis a interdit à un fabricant d'applications de proposer des stalkerwares. C'était la toute première interdiction de ce type.

Le 17 août 2021, le Bundestag allemand a voté la loi « Act to Amend the Criminal Code - More Effective Combating of Stalking and Better Coverage of Cyberstalking » (traduit de l'allemand. En français : Amendement du code criminel : lutte plus efficace contre les stalkerwares et meilleure couverture du suivi en ligne). La nouvelle loi est entrée en vigueur le 1er octobre 2021 et inclut désormais le suivi en ligne dans la liste des infractions. Ce changement s'explique par l'évolution technologique continue et l'essor associé du harcèlement en ligne, notamment au moyen d'applications de suivi ou stalkerwares. En outre, une partie importante de la nouvelle loi classifie un cas comme sérieux si l'agresseur « utilise, au cours d'une infraction, un programme informatique qui vise à espionner numériquement d'autres personnes ».

Le Conseil de l'Europe s'est montré très actif sur ce sujet en 2021. Dans ses premières recommandations sur la « dimension numérique » de la violence faite aux femmes, le groupe GREVIO du Conseil de l'Europe définit et souligne les problèmes de violence basée sur le genre perpétrés en ligne et les attaques informatisées visant les femmes, comme les appareils de géolocalisation légaux qui permettent aux agresseurs de suivre leurs victimes. En décembre 2021, un rapport d'initiative législative sur la cyberviolence basée sur le genre a été adopté par le Parlement européen. Le rapport propose (i) une définition commune de la cyberviolence faite aux femmes et (ii) un renforcement des capacités des acteurs. Il évoque les stalkerwares parmi les principales méthodes de cyberviolence et « révoque la notion selon laquelle les applications de stalkerware peuvent être

considérées comme des applications de contrôle parental ». Suivant les recommandations générales du Conseil de l'Europe, ce rapport, même s'il n'est pas contraignant, est un autre document officiel positif mettant en exergue le problème des stalkerwares et incitant les États européens à adapter leur législation et leurs mesures pour lutter contre ce fléau. Enfin, le 8 mars dernier, la Commission européenne a publié une proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique. Ce document couvre la cyberviolence et dédie deux articles au suivi en ligne (article 8) et au cyberharcèlement (article 9), qu'il propose de traiter comme un crime.

Vous pensez être suivi(e) par un stalkerware ? Voici quelques conseils

Si vous avez besoin d'aide, contactez une organization de soutien locale. Pour en trouver une proche de vous, consultez le site de la Coalition contre les stalkerwares

Que vous soyez ou non victime, voici quelques conseils à suivre pour mieux vous protéger :

- Protégez votre téléphone avec un mot de passe fort à ne jamais partager avec votre partenaire, vos amis ou vos collègues.
- Changez régulièrement les mots de passe de vos comptes et ne les partagez avec personne.
- Téléchargez uniquement des applications provenant de sources officielles comme Google Play ou l'Apple App Store.
- Installez une solution de sécurité informatique fiable comme Kaspersky Internet Security pour Android sur vos appareils et analysez-les régulièrement. Toutefois, si un stalkerware est déjà installé, cela ne doit être fait qu'après l'évaluation du risque auquel s'expose la victime, car l'agresseur peut remarquer l'utilisation d'une solution de cybersécurité.

Les victimes de stalkerwares peuvent être victimes d'un cycle plus important d'abus, y compris physiques. Dans certains cas, l'agresseur est informé si sa victime analyse son appareil ou supprime une application de stalkerware. Cela peut alors mener à des agressions supplémentaires et à une escalade de la violence. C'est pourquoi il est important de procéder avec vigilance si vous pensez être la cible d'un stalkerware.

- **Contactez une organisation locale d'aide aux victimes :** pour en trouver une près de chez vous, consultez le site Web de la Coalition contre les stalkerware (Coalition Against Stalkerware).
- **Guettez les signes suivants : i**l peut s'agir du niveau de votre batterie qui baisse rapidement en raison d'applications inconnues ou suspectes, d'applications récemment installées avec un accès pour utiliser et suivre votre localisation, envoyer ou recevoir des SMS et autres activités personnelles. Vérifiez également si votre paramètre de « sources inconnues » est activé. Cela peut signaler qu'un logiciel indésirable a été installé par une source tierce. Il est important de noter que les signes ci-dessus ne sont que des symptômes d'une éventuelle installation de stalkerware, et non une indication définitive.
- **N'essayez pas de supprimer le stalkerware, de modifier des paramètres ni de trafiquer votre téléphone :** votre agresseur potentiel pourrait être alerté et la situation pourrait empirer. Vous risquez également de supprimer des données importantes ou des preuves susceptibles d'être utilisées dans le cadre d'une poursuite judiciaire.

Pour plus d'information sur nos activités sur le sujet des stalkerwares ou pour toute autre demande, merci de nous écrire à ExtR@kaspersky.com.

La Coalition Against Stalkerware a été fondée en novembre 2019 en réponse à la menace croissante des stalkerwares. La Coalition cherche à associer l'expertise de ses partenaires en matière de soutien aux victimes d'actes de violence domestique, de prise en charge des auteurs de ces actes et de défense des droits numériques dans le but de lutter contre les comportements criminels liés aux stalkerwares. Tous les membres s'engagent à lutter contre la violence domestique et le harcèlement en luttant contre l'utilisation des stalkerwares et en sensibilisant le public à ce problème.

La Coalition contre les stalkerware :
https://stopstalkerware.org/

COALITION AGAINST STALKERWARE

Nouvelles sur les cyber menaces: www.securelist.com
Nouvelles sur la sécurité informatique:
business.kaspersky.com
Sécurité informatique pour les PME:
www.kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les grandes entreprises:
www.kaspersky.fr/enterprise-security

www.kaspersky.fr

kaspersky