L'état des **stalkerwares** en 2022

Coalition Against Stalkerware

kaspersky

Contenu

Principales conclusions de 2022

Les tendances 2022 observées par Kaspersky

- Méthodologie
- Chiffres de détection à l'échelle mondiale : utilisateurs touchés
- Chiffres de détection à l'échelle mondiale et régionale : géographie des utilisateurs touchés
- Chiffres de détection à l'échelle mondiale – applications de stalkerware

Harcèlement numérique et violence sexiste

Ensemble, continuons à lutter contre les stalkerwares

Vous pensez être victime d'un stalkerware ? Voici quelques conseils…

Principales conclusions de 2022

The State of Stalkerware est un rapport annuel de Kaspersky qui permet de mieux comprendre combien de personnes dans le monde sont touchées par le harcèlement numérique. Le stalkerware est un logiciel disponible dans le commerce qui peut être installé discrètement sur des smartphones, permettant aux auteurs de surveiller la vie privée d'une personne à son insu.

Les stalkerwares peuvent être téléchargés et facilement installés par toute personne disposant d'une connexion Internet et d'un accès physique à un smartphone. L'auteur enfreint la vie privée de la victime dans la mesure où il peut ensuite utiliser le logiciel pour surveiller d'énormes volumes de données personnelles. Selon le type de logiciel, il est généralement possible de vérifier la localisation de l'appareil, les messages texte, les discussions sur les réseaux sociaux, les photos, l'historique du navigateur et plus encore. Les stalkerwares fonctionnent en arrière-plan, ce qui signifie que la plupart des victimes ne sont pas conscientes que leurs moindres actions sont surveillées.

Dans la plupart des pays du monde, l'utilisation de stalkerwares n'est actuellement pas interdite. En revanche, l'installation d'une telle application sur le smartphone d'un tiers sans son consentement est illégale et punissable. Toutefois, c'est l'auteur de l'infraction qui en sera tenu responsable, et non le développeur de l'application.

Avec d'autres technologies connexes, les stalkerwares font partie des abus liés à la technologie et sont souvent utilisés dans les relations conflictuelles. Comme il s'agit d'un problème plus vaste, Kaspersky collabore avec des experts et des organisations compétentes dans le domaine de la violence domestique, allant des services d'aide aux victimes et des programmes pour les auteurs de violence à la recherche et aux agences gouvernementales, afin de partager les connaissances, et de soutenir les professionnels et les victimes.

Données marquantes de 2022

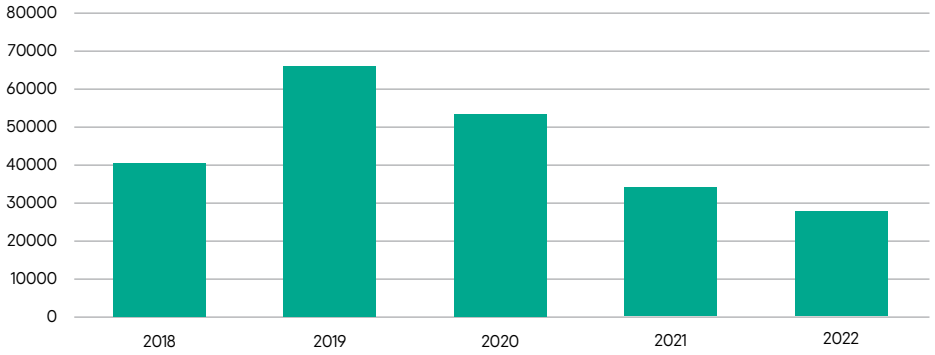
- **En 2022, les données de Kaspersky indiquent que 29 312 individus uniques dans le monde ont été touchés par un stalkerware.** Par rapport à la tendance baissière enregistrée les années précédentes, ce chiffre est semblable au nombre total d'utilisateurs concernés en 2021. En tenant compte des développements des stalkerwares au cours des dernières années, les données suggèrent une tendance à la stabilisation. Plus largement, il est important de noter que les données couvrent le nombre d'utilisateurs concernés utilisant Kaspersky. Le nombre de personnes touchées à l'échelle mondiale est probablement beaucoup plus élevé. Il se peut que certains utilisateurs concernés utilisent une autre solution de cybersécurité sur leurs appareils, tandis que d'autres n'utilisent aucune solution du tout.
- **En outre, les données révèlent une prolifération stable des stalkerwares au cours des 12 mois de l'année 2022.** En moyenne, 3 333 utilisateurs par mois ont été touchés par un stalkerware pour la première fois. La stabilité du taux de détection indique que le harcèlement numérique est devenu un problème persistant qui mérite une plus grande attention de la part de la société. Les membres de la Coalition Against Stalkerware évaluent à près d'un million le nombre de victimes de stalkerware dans le monde chaque année.
- Selon le Kaspersky Security Network, les **stalkerwares sont le plus souvent utilisés en Russie, au Brésil et en Inde**, mais il s'agit d'un phénomène mondial qui touche tous les pays. Sur le plan régional, les données révèlent que le plus grand nombre d'utilisateurs touchés se trouve dans les pays suivants :
  - Allemagne, Italie et France (Europe) ;
  - Iran, Turquie et Arabie saoudite (Moyen-Orient et Afrique) ;
  - Inde, Indonésie et Australie (Asie-Pacifique) ;
  - Brésil, Mexique et Équateur (Amérique latine) ;
  - États-Unis (Amérique du Nord) ;
  - Russie, Kazakhstan et Biélorussie (Europe de l'Est (à l'exception des pays de l'Union européenne), Russie et Asie centrale).
- Au niveau mondial, l'application de harcèlement la plus utilisée est Reptilicus, qui a touché 4 065 touchés.

Les tendances 2022 observées par Kaspersky

En 2022, un total de 29 312 utilisateurs uniques ont été touchés par des stalkerwares

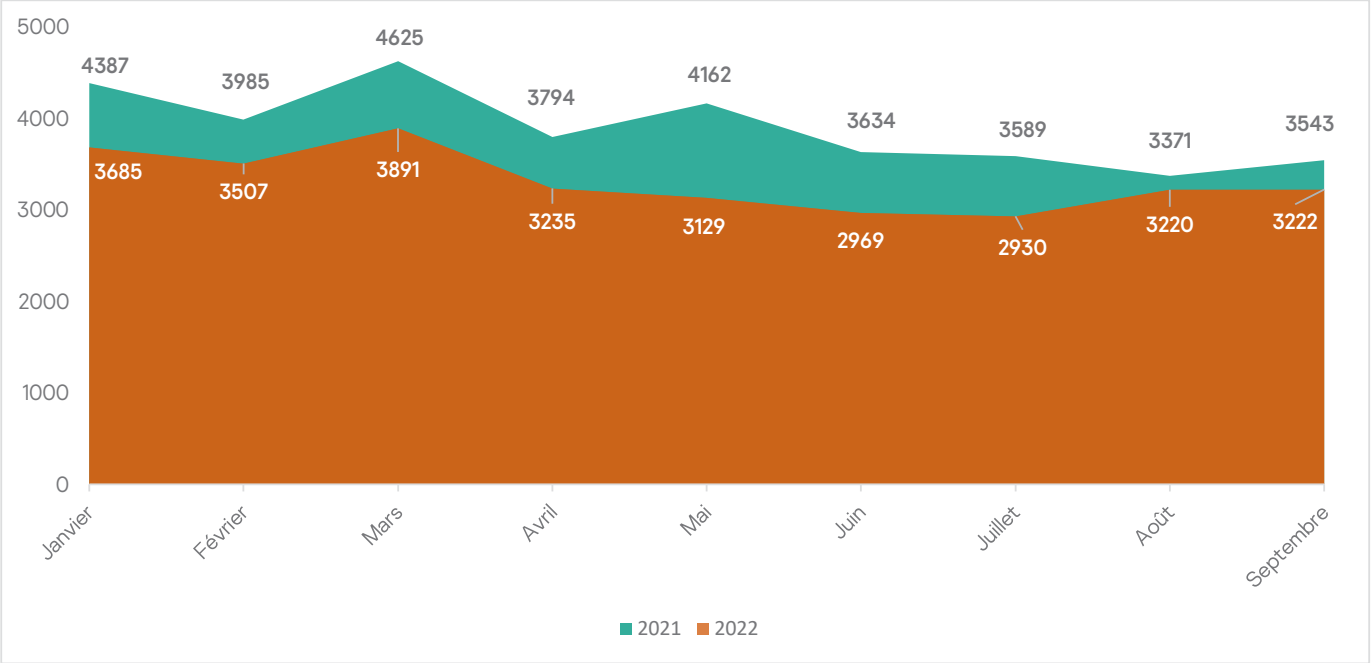
Chiffres de détection à l'échelle mondiale : utilisateurs touchés

Cette section compare les statistiques mondiales et régionales collectées par Kaspersky en 2022 avec les statistiques des années précédentes. En 2022, ce sont au total 29 312 utilisateurs uniques qui ont été touchés par les stalkerwares. Le graphique 1, ci-dessous, présente la variation de ce nombre d'année en année depuis 2018.



Graphique 1 – Évolution des utilisateurs touchés d'une année à l'autre depuis 2018

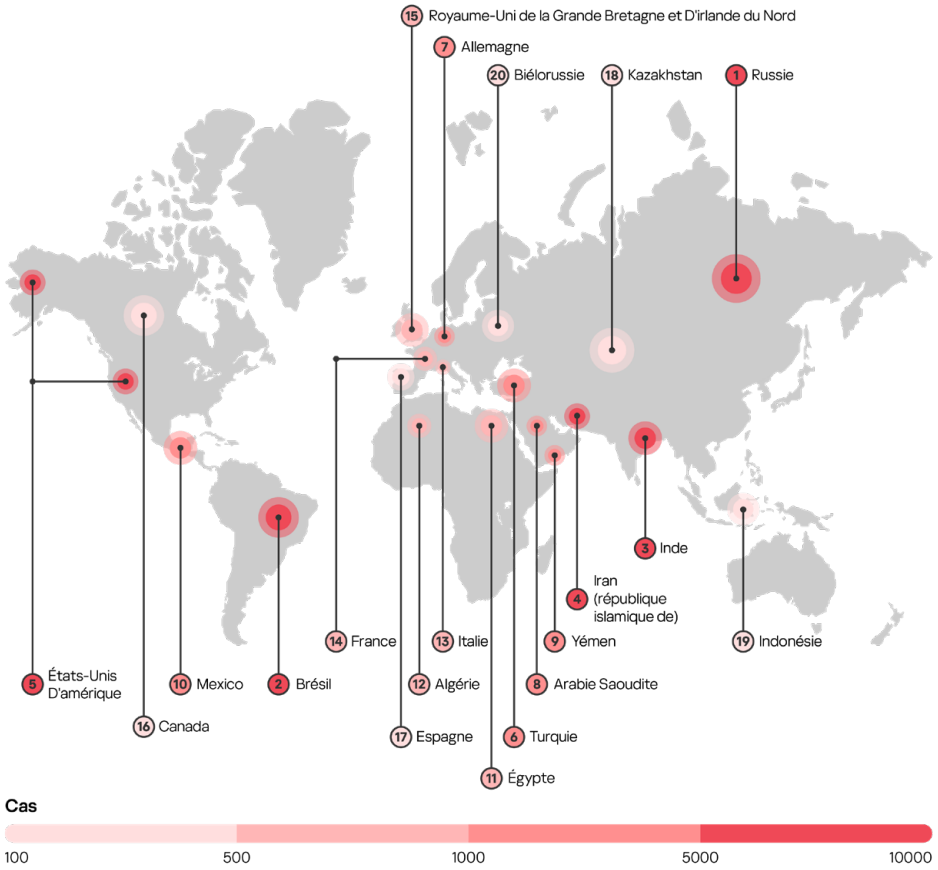
Le graphique 2, ci-dessous, présente le nombre d'utilisateurs uniques touchés par mois entre 2021 et 2022. En 2022, la situation est presque identique à celle de 2021, ce qui indique que le taux de prolifération des stalkerwares s'est stabilisé. En moyenne, 3 333 utilisateurs ont nouvellement été touchés par des stalkerwares chaque mois.



Graphique 2 – Utilisateurs uniques touchés par mois au cours de la période 2021-2022

Chiffres de détection à l'échelle mondiale et régionale : géographie des utilisateurs touchés

La question des stalkerwares reste un problème mondial. En 2022, Kaspersky a recensé des utilisateurs concernés dans 176 pays.



Carte 1 – Les pays les plus touchés par les stalkerwares en 2022

Méthodologie

Les données contenues dans ce rapport proviennent de statistiques agrégées sur les menaces obtenues auprès de Kaspersky Security Network. Kaspersky Security Network se consacre au traitement des flux de données de télémétrie provenant de millions de participants bénévoles du monde entier. Toutes les données reçues sont rendues anonymes. Pour calculer les statistiques, la gamme grand public des solutions de sécurité mobile de Kaspersky a été évaluée selon les critères de détection des stalkerwares établis par la Coalition Against Stalkerware. Cela signifie que le nombre d'utilisateurs concernés a été ciblé uniquement par des stalkerwares. Les autres types d'applications de surveillance ou de logiciels espions qui ne correspondent pas à la définition de la Coalition ne sont pas inclus dans les statistiques du rapport.

Les statistiques reflètent les utilisateurs mobiles uniques touchés par les stalkerwares, ce qui est différent du nombre total de détections. Le nombre de détections peut être plus élevé, car un stalkerware peut avoir été détecté plusieurs fois sur le même appareil du même utilisateur unique si ce dernier a décidé de ne pas supprimer l'application après avoir reçu une notification.

Enfin, les statistiques reflètent seulement les utilisateurs mobiles qui utilisent les solutions de sécurité informatique de Kaspersky. Il se peut que certains utilisateurs utilisent une autre solution de cybersécurité sur leurs appareils, tandis que d'autres n'utilisent aucune solution du tout.

En 2022, la Russie (8 281), le Brésil (4 969) et l'Inde (1 807) étaient les 3 pays comptant le plus d'utilisateurs touchés. Selon les statistiques de Kaspersky, ces trois pays restent en tête depuis 2019. Par rapport aux années précédentes, il convient de noter que le nombre d'utilisateurs concernés aux États-Unis a baissé dans le classement et figure désormais à la cinquième place avec 1 295 utilisateurs touchés. À l'inverse, une augmentation a été constatée en Iran qui est passé à la quatrième place avec 1 754 utilisateurs touchés.

Toutefois, par rapport à 2021, seul l'Iran fait son entrée dans le top 5 des pays les plus touchés. Les quatre autres pays – la Russie, le Brésil, l'Inde et les États-Unis – figurent habituellement en tête de liste. Si l'on examine l'autre moitié du top 10 des pays les plus atteints, la Turquie, l'Allemagne et le Mexique sont restés parmi les pays les plus touchés par rapport à l'année dernière. Les nouveaux entrants dans le top 10 des pays les plus touchés en 2022 sont l'Arabie saoudite et le Yémen.

	Pays	Utilisateurs touchés
1	Russie	281 8
2	Brésil	969 4
3	Inde	807 1
4	Iran	754 1
5	États-Unis d'Amérique	295 1
6	Turquie	755
7	Allemagne	736
8	Arabie saoudite	612
9	Yémen	527
10	Mexique	474

Tableau 1 – Les 10 pays les plus touchés par les stalkerwares dans le monde en 2022

En Europe, le nombre total d'utilisateurs uniques touchés en 2022 était de 3 158. Les trois pays les plus touchés en Europe ont été l'Allemagne (737), l'Italie (405) et la France (365). Par rapport à 2021, tous les pays jusqu'à y compris la septième place de la liste (les Pays-Bas) continuent de faire partie des pays les plus touchés en Europe. Les nouveaux entrants dans la liste sont la Suisse, l'Autriche et la Grèce.

	Pays	Utilisateurs touchés
1	Allemagne	736
2	Italie	405
3	France	365
4	Royaume-Uni	313
5	Espagne	296
6	Pologne	220
7	Pays-Bas	154
8	Suisse	123
9	Autriche	71
10	Grèce	70

Tableau 2 – Les 10 pays les plus touchés par les stalkerwares en Europe en 2022

En Europe de l'Est (à l'exclusion des pays de l'Union européenne), en Russie et en Asie centrale, le nombre total d'utilisateurs uniques touchés en 2022 était de 9 406. Les trois principaux pays étaient la Russie, le Kazakhstan et la Biélorussie.

	Pays	Utilisateurs touchés
1	Russie	281 8
2	Kazakhstan	296
3	Biélorussie	267
4	Ukraine	258
5	Azerbaïdjan	130
6	Ouzbékistan	76
7	Moldavie	34
8	Tadjikistan	32
9	Kirghizistan	31
10	Arménie	27

Tableau 3 – Les 10 pays les plus touchés par les stalkerwares en Europe de l'Est (hors pays de l'UE), en Russie et en Asie centrale en 2022

Dans la région du Moyen-Orient et de l'Afrique, le nombre total d'utilisateurs touchés était de 6 330, soit un peu plus qu'en 2021. Si l'Iran, avec 1 754 utilisateurs touchés, figure en tête de cette liste en 2022, la Turquie, avec 755 utilisateurs touchés, se hisse à la deuxième place dans la région, suivie de près par l'Arabie saoudite avec 612 utilisateurs touchés.

	Pays	Utilisateurs touchés
1	Iran	754 1
2	Turquie	755
3	Arabie saoudite	612
4	Yémen	527
5	Égypte	469
6	Algérie	407
7	Maroc	168
8	Émirats arabes unis	155
9	Afrique du Sud	145
10	Kenya	123

Tableau 4 – Les 10 pays les plus touchés par les stalkerwares au Moyen-Orient et en Afrique en 2022

Dans la région Asie-Pacifique, le nombre total d'utilisateurs touchés était de 3 187. L'Inde reste

loin devant les autres pays de la région, avec 1 807 utilisateurs touchés. L'Indonésie occupe la deuxième place avec 269 utilisateurs touchés, tandis que l'Australie arrive en troisième position avec 190 utilisateurs touchés.

	Pays	Utilisateurs touchés
1	Inde	807 1
2	Indonésie	269
3	Australie	190
4	Philippines	134
5	Malaisie	129
6	Vietnam	109
7	Bangladesh	105
8	Japon	95
9	Thaïlande	52
10	Pakistan	48

Tableau 5 – Les 10 pays les plus touchés par les stalkerwares dans la région Asie-Pacifique en 2022

La région Amérique latine et Caraïbes reste dominée par le Brésil avec 4 969 utilisateurs touchés. Il s'agit d'environ 32 % du nombre total d'utilisateurs touchés dans la région. Le Brésil est suivi par le Mexique et l'Équateur dans la liste, tandis que la Colombie est passée à la quatrième place. Au total, 6 170 utilisateurs touchés ont été recensés dans la région.

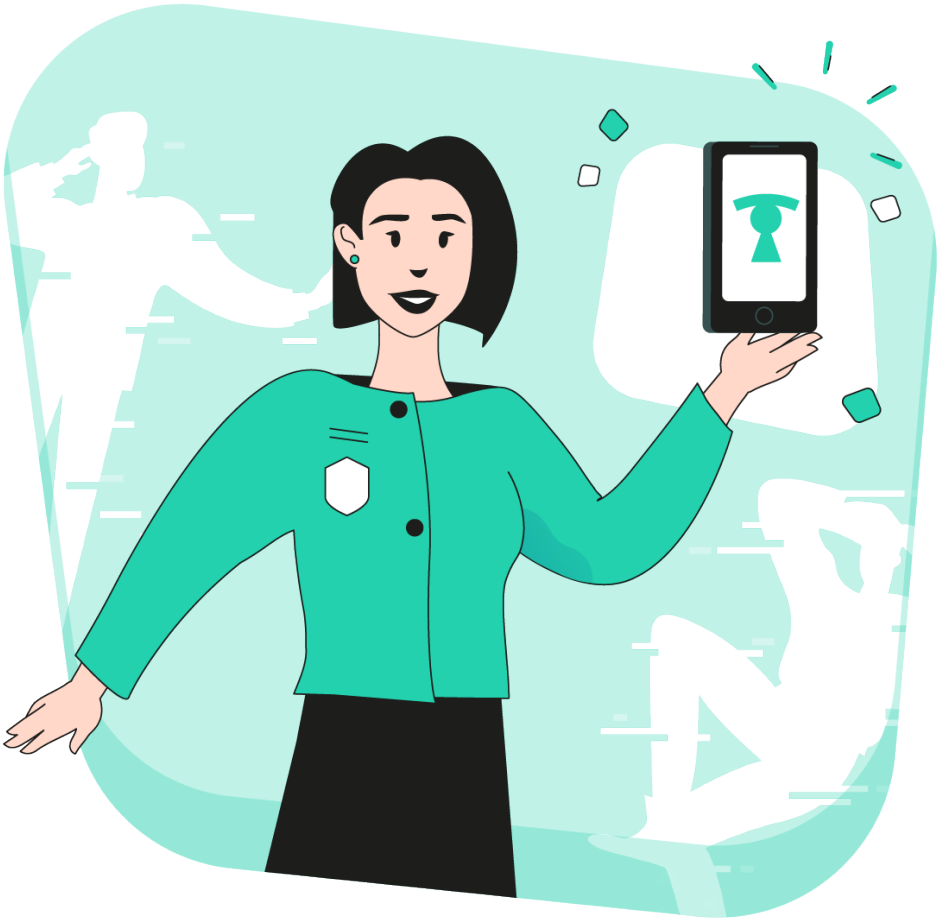
	Pays	Utilisateurs touchés
1	Brésil	969 4
2	Mexique	474
3	Équateur	146
4	Colombie	120
5	Pérou	111
6	Argentine	85
7	Chili	49
8	Bolivie	32
9	Venezuela	30
10	République dominicaine	24

Tableau 6 – Les 10 pays les plus touchés par les stalkerwares en Amérique latine en 2022

Enfin, en Amérique du Nord, 87 % de tous les utilisateurs touchés dans la région se trouvent aux États-Unis. Il faut s'y attendre compte tenu de la taille relative de la population aux États-Unis par rapport au Canada. Dans la région de l'Amérique du Nord, 1 585 utilisateurs ont été touchés au total.

	Pays	Utilisateurs touchés
1	États-Unis d'Amérique	295 1
2	Canada	299

Tableau 7 – Nombre d'utilisateurs touchés par les stalkerwares en Amérique du Nord en 2022



Les appareils fonctionnant sous Android et iOS sont-ils concernés de la même manière par les stalkerware ?

Les outils de stalkerware sont moins fréquents sur les iPhone que sur les appareils Android parce qu'iOS est par définition un système fermé. Toutefois, les auteurs d'infractions peuvent contourner cette limitation sur les iPhone « débridés » (« jailbreakés »), mais pour les débrider, ils doivent quand même avoir un accès physique direct au téléphone. Les utilisateurs d'iPhone qui craignent de se faire surveiller devraient toujours garder un œil sur leur appareil.

Un malfaiteur peut également offrir à sa victime un iPhone (ou tout autre appareil) sur lequel est préinstallé un stalkerware. De nombreuses entreprises proposent ces services en ligne, permettant aux malfaiteurs de faire installer ces outils sur des téléphones neufs, qui peuvent ensuite être livrés dans un emballage d'usine sous forme de cadeau à la victime ciblée.

Chiffres de détection à l'échelle mondiale – applications de stalkerware

Cette section dresse la liste des applications de stalkerware les plus couramment utilisées pour contrôler les smartphones dans le monde entier. En 2022, l'application la plus populaire était Reptilicus (4 065 utilisateurs touchés). Cette année, Kaspersky a détecté 182 applications de stalkerware différentes.

	Nom de l'application	Utilisateurs touchés
1	Reptilicus (aussi appelé Vkurse)	065 4
2	Cerberus	407 2
3	KeyLog	721 1
4	MobileTracker	633 1
5	wSpy	342 1
6	SpyPhone	211 1
7	Anlost	189 1
8	Track My Phones	137 1
9	MonitorMinor	864
10	Hovermon	827

Tableau 8 – Liste des 10 principales applications de stalkerware en 2022

Les stalkerwares permettent de prendre le contrôle de la vie d'une victime. Leurs fonctionnalités varient selon le type d'application et suivant qu'elle a été payée ou acquise gratuitement. En règle générale, les stalkerwares se font passer pour des applications antivol ou de contrôle parental légitimes, alors qu'ils sont en réalité très différents, notamment en raison de leur installation sans consentement ni notification à la personne suivie, et de leur fonctionnement en mode furtif sur les smartphones. Below are some of the most common functions that may be present in stalkerware applications:

Vous trouverez ci-dessous quelques-unes des fonctionnalités les plus courantes que l'on retrouve dans les applications de stalkerware :

- Masquage de l'icône de l'application
- Lecture des SMS, des MMS et des journaux d'appels
- Récupération des listes de contacts
- Suivi de la localisation GPS
- Suivi des événements du calendrier
- Lecture de messages provenant de services de messagerie et de réseaux sociaux populaires, tels que 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.
- Consultation des photos et des images dans les galeries d'images des téléphones
- Création de captures d'écran
- Prise de photos avec la caméra frontale (mode selfie)

Harcèlement numérique et violence sexiste

Les stalkerwares, une méthode de cyberharcèlement qui fait partie de la violence numérique.

Aussi bien les femmes que les hommes peuvent être victimes de violence numérique, mais les recherches démontrent que dans l'écrasante majorité des cas, les femmes sont ciblées en raison de leur sexe. Il est important de se rappeler que la violence numérique constitue une autre dimension de la violence. Elle doit être comprise comme un prolongement de la violence hors ligne, car elle a des effets réels et négatifs sur les victimes. Pour en savoir plus, veuillez lire la fiche d'information « La cyberviolence contre les femmes et les filles : Termes et concepts clés » (2022) publié par l'Institut européen pour l'égalité entre les hommes et les femmes.

Des experts du monde universitaire et des organisations de la société civile travaillant dans le domaine des services d'aide aux victimes et des programmes destinés aux auteurs de violences partagent avec nous leur expérience et leurs points de vue sur la violence numérique liée au genre et sur les abus technologiques en général.

L'importance des données pour comprendre l'ampleur de la violence numérique – Dr Leonie Maria Tanczer, professeur associé à l'University College London et chef du groupe de recherche sur le genre et la technologie de l'UCL

Les recherches antérieures sur les formes de harcèlement et de violence sexiste facilitées par la technologie se sont concentrées sur des systèmes numériques "de tous les jours" qui peuvent contraindre, contrôler et nuire à une personne ou à des groupes d'individus. Alors que le rapport et les données actuels se limitent aux appareils mobiles, le harcèlement numérique peut être facilité par divers appareils, notamment les traceurs GPS ou ce que l'on appelle "l'Internet des objets" (IoT). Ceci inclut des produits connectés tels que des sonnettes intelligentes, des caméras de vidéosurveillance ou des haut-parleurs.

Les données factuelles sur les abus liés à la technologie sont également encore très limitées. Les centres de recherche actuels se trouvent principalement en Australie, au Royaume-Uni et aux États-Unis. La plupart des études se concentrent donc sur les données provenant de ces pays, ce qui crée des angles morts. Des données telles que celles présentées dans ce rapport contribuent à une compréhension plus large du paysage de la maltraitance technologique, ce qui est nécessaire de toute urgence.

Il a également été démontré que les services d'aide aux victimes ont du mal à répondre aux exigences croissantes de mise à jour des développements technologiques. Ils ont réclamé des ajouts aux pratiques existantes en matière d'évaluation des risques et de sécurité, notamment des "plans d'action contre le cyberharcèlement" et des formations spécifiques afin d'accroître les capacités et la réactivité du secteur. En effet, des offres de services de plus en plus spécialisées sont proposées, comme en témoignent l'équipe Tech Safety de l'association Refuge, le Safety Net Project du National Network to End Domestic Violence (NNEDV) ou la Clinic to End Tech Abuse (CETA).

Le Groupe de Recherche sur le Genre et la Technologie de l'University College London (UCL) étudie les points d'intersection entre la technologie, la sécurité et le genre afin que les systèmes numériques fonctionnent pour tous. Pour en savoir plus :

https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

Prêter plus d'attention à ceux qui souffrent de la violence numérique – Elena Gajotto, vice-présidente de Una Casa Per L'Uomo

Le cyberharcèlement a un impact concret dans la vie réelle de ceux qui le subissent. Il y a des effets psychologiques, physiques et sociaux à moyen et long terme que nous constatons quotidiennement dans nos centres anti-violence. Comme le souligne le Service de recherche du Parlement européen dans son étude (2021), toutes les femmes peuvent être des victimes potentielles de cyberharcèlement, qu'il s'agisse de personnalités publiques, d'ex-partenaires ou de simples utilisatrices de médias sociaux. Le cyberharcèlement englobe différents types de comportements tels l'envoi persistant de messages, la surveillance de l'activité d'une victime ou d'autres formes de poursuite en ligne, et comme l'indique la même étude, "il se peut que le cyberharcèlement soit simplement un outil supplémentaire dans la boîte à outils du harceleur".

Lorsque l'on travaille sur la violence numérique, il faut prendre en compte les caractéristiques suivantes :

- La violence numérique peut être perpétrée en même temps que d'autres formes de violence (physique, sexuelle, psychologique, économique, etc.).
- La violence peut commencer en ligne et se poursuivre hors ligne ou, à l'inverse, elle peut commencer dans le monde hors ligne et se poursuivre dans la sphère numérique.
- Il n'est pas simple de supprimer - de manière permanente - les contenus offensants, violents ou déclencheurs publiés en ligne.
- Les auteurs de la violence numérique peuvent être des individus ou des groupes, et peuvent être connus ou non de la victime.
- La violence numérique peut être exercée au moyen d'un large éventail d'appareils (PC, smartphones, appareils domestiques intelligents, etc.) et sur de nombreuses plateformes différentes (sites web, applications de messagerie instantanée, chats en ligne, médias sociaux, etc.)

Comme indiqué précédemment, bien qu'elles se déroulent dans la sphère numérique, ces formes de violence ont un impact profond sur la vie des victimes. Des études montrent que les femmes sont les principales victimes de cyberharcèlement ou d'autres formes de violence numérique. Elles présentent de nombreux symptômes similaires à ceux des victimes de la violence hors ligne, tels que l'anxiété, les crises de panique, le syndrome de stress post-traumatique, les pensées suicidaires, la colère, le manque de confiance en soi et les difficultés de concentration. Il peut également y avoir des effets négatifs économiques (extorsion, perte de revenus, etc.) et relationnels (perte du réseau familial et amical, isolement social, etc.). En outre, la violence numérique a un impact collectif, tant au niveau économique que politique, avec d'une part une augmentation des coûts publics juridiques, administratifs et sanitaires, et d'autre part une moindre participation des femmes au discours public.

Il est donc important de souligner le danger de ce phénomène. La société doit accorder plus d'attention aux victimes de la violence numérique. À cette fin, nous travaillons avec nos membres ainsi qu'avec Kaspersky et tous les partenaires de la Coalition Against Stalkerware pour soutenir les victimes et mieux former les professionnels travaillant dans le domaine de la violence domestique.

Una Casa Per L'Uomo est une organisation de la société civile italienne qui gère des services d'aide aux victimes. Una Casa Per L'Uomo a été un partenaire du consortium du projet DeStalk (2021-2023), cofinancé par le programme Droits, égalité et citoyenneté de l'Union européenne, et est membre de la Coalition Against Stalkerware.

S'attaquer aux attitudes sociales qui favorisent les abus facilités par la technologie – Anna McKenzie, responsable de la communication au WWP EN

Les abus facilités par la technologie, tels que les logiciels d'espionnage ou stalkerwares, sont une préoccupation croissante pour nos organisations membres qui travaillent sur le changement de comportement des auteurs de violences domestiques.

La violence numérique continue d'augmenter : les appareils numériques, les logiciels de surveillance secrets et les espaces en ligne offrent aux partenaires violents l'environnement idéal pour étendre leur contrôle sur la vie de leur partenaire. Cependant, vérifier le téléphone de son partenaire, lire ses e-mails, savoir où il se trouve et connaître ses mots de passe est aujourd'hui si courant que les individus ne se rendent souvent pas compte qu'ils adoptent des comportements abusifs.

Comment se fait-il que ces atteintes apparentes à la vie privée ne soient pas perçues comme telles ?

En 2021, Kaspersky a publié le "Digital Stalking in Relationships Report", mettant en lumière certaines tendances inquiétantes. Selon les données, des comportements tels que la surveillance des activités numériques d'un partenaire avec son consentement étaient largement considérés comme acceptables pour assurer la transparence au sein d'une relation. Il est toutefois inquiétant de constater que près d'un tiers des personnes interrogées acceptent de surveiller les activités d'un partenaire sans son consentement, surtout si elles pensent que celui-ci est infidèle.

Ces attitudes renvoient directement aux problèmes que nos membres rencontrent régulièrement dans leur travail avec les auteurs de violences domestiques. Il est très problématique de supposer qu'une personne ne consentant pas au contrôle signifie qu'elle cache une possible infidélité. Dans les relations abusives, le consentement est au mieux ténu : Comment peuvent-ils dire oui, s'ils ne peuvent pas dire non, après tout ? De même, l'acceptation du soupçon d'infidélité comme excuse pour espionner un partenaire est une occasion en or pour les partenaires abusifs qui perçoivent constamment une menace de tromperie dans leur relation. Cela témoigne également d'un sentiment d'appropriation et d'un manque de communication saine, qui sont des préoccupations centrales dans les relations abusives.

Nous pensons qu'au-delà du besoin évident de réglementation juridique, de renforcement des capacités et de sensibilisation générale à la question de la violence numérique, il est de la plus haute importance que les attitudes favorables aux abus facilités par la technologie soient abordées de manière généralisée et dès le plus jeune âge. Des études telles que le rapport State of Stalkerware constituent un contrôle important du statu quo, mais nous devons faire davantage pour le changer. Avec la campagne #NoExcuse4Abuse, développée et mise en œuvre en coopération avec Kaspersky, nous avons fait un premier pas vers la lutte contre les attitudes sociales néfastes envers les abus facilités par la technologie et les logiciels de harcèlement.

Le WWP EN est un réseau européen qui compte 69 membres issus de 34 pays. Nous pensons que sans une approche permettant de cibler les auteurs de violence domestique et de les tenir pour responsables, toute stratégie visant à mettre fin à la violence entre partenaires intimes est incomplète. Notre travail se concentre sur l'arrêt de la violence des hommes, leur responsabilisation et la promotion de la Convention d'Istanbul. Pour en savoir plus :

https://www.work-with-perpetrators.eu

Ensemble, continuons à lutter contre les stalkerwares

Les stalkerwares ne sont avant tout pas un problème technique, mais l'expression d'un problème de société qui nécessite des actions dans tous les domaines de la société. Kaspersky s'engage non seulement à protéger activement les utilisateurs contre cette menace, mais aussi à maintenir un dialogue à plusieurs niveaux avec des organisations à but non lucratif, ainsi qu'avec des organismes du milieu industriel, de la recherche et du secteur public du monde entier, afin de collaborer à l'élaboration de solutions permettant de faire face à ce problème.

En 2019, Kaspersky a été la première entreprise de cybersécurité du secteur à développer un nouveau type d'alerte pour attirer l'attention et avertir clairement les utilisateurs si un stalkerware a été trouvé sur leur appareil. Alors que les solutions de Kaspersky signalent depuis de nombreuses années les applications potentiellement dangereuses qui ne sont pas des programmes malveillants (y compris les stalkerwares) la nouvelle notification avertit l'utilisateur qu'une application a été trouvée sur son appareil et qu'elle est susceptible de l'espionner.

En 2022, dans le cadre du lancement par Kaspersky d'un nouveau portefeuille de produits grand public, l'alerte de confidentialité a été étendue et informe désormais l'utilisateur de la présence d'un stalkerware sur l'appareil, mais l'avertit également que s'il supprime le stalkerware, la personne qui a installé l'application sera prévenue. Cette action pourrait aggraver la situation. De plus, l'utilisateur risque d'effacer des données ou des preuves importantes qui pourraient être utilisées dans le cadre d'une poursuite judiciaire. L'illustration n° 2, ci-dessous, présente le nouvel avertissement dans l'encadré bleu. L'alerte de confidentialité de Kaspersky est incluse dans toutes les solutions de sécurité grand public proposées par l'entreprise pour assurer une protection contre les stalkerwares.

En 2019, Kaspersky a également cofondé Coalition Against Stalkerware, un groupe de travail international contre les stalkerwares et la cyber-violence domestique qui réunit des entreprises informatiques privées, des ONG, des institutions de recherche ainsi que des organismes d'application de la loi qui luttent contre le cyberharcèlement et aident les victimes d'abus en ligne. Grâce à un consortium de plus de 40 organisations, les parties prenantes peuvent partager leur expertise et travailler de concert pour trouver une solution au problème de la violence en ligne. En outre, le site de la Coalition, qui est disponible en 7 langues différentes, fournit aux victimes une aide et des conseils dans le cas où elles soupçonneraient la présence de stalkerware sur leurs appareils.

De 2021 à 2023, Kaspersky a été un partenaire de consortium du projet de l'UE DeStalk, cofinancé par le programme Citoyens, Egalité, Droits et Valeurs de l'Union européenne. Les cinq partenaires du projet qui ont formé le consortium ont combiné l'expertise de la communauté de la sécurité informatique, de la recherche, des organisations de la société civile et des autorités publiques. En conséquence, le projet DeStalk a formé un total de 375 professionnels travaillant directement dans les services d'assistance aux femmes et les programmes pour les auteurs de violences, ainsi que des fonctionnaires des autorités publiques, sur la manière de faire face efficacement aux stalkerwares et autres formes numériques de violence basée sur le genre, ainsi que sur la sensibilisation du public à la violence numérique et aux stalkerwares.

Dans le cadre du projet, Kaspersky a développé une formation en ligne sur la cyberviolence et les stalkerwares basé sur Kaspersky Automated Security Awareness Platform, une plateforme de formation en ligne gratuite proposée dans cinq langues différentes. À ce jour, plus de 130 professionnels ont suivi la formation en ligne et 80 autres y participent actuellement. Bien que le projet DeStalk soit arrivé à son terme, la formation en ligne est toujours disponible sur le site Internet du projet DeStalk https://www.work-with-perpetrators.eu/destalk.

En juin 2022, Kaspersky a lancé un site dédié à TinyCheck pour faire connaître davantage l'outil. TinyCheck est un outil open source gratuit, sûr et ouvert qui peut être utilisé par les organisations à but non lucratif et les unités de police pour aider les victimes de harcèlement numérique. En 2020, l'outil a été créé pour vérifier la présence de stalkerwares et d'applications de surveillance sur un smartphone ou autre appareil, rapidement et de manière non invasive. Il ne doit pas être installé sur l'appareil de l'utilisateur et fonctionne de manière autonome pour éviter d'être détecté par un harceleur. TinyCheck analyse le trafic sortant d'un appareil à l'aide d'une connexion Wi-Fi ordinaire et détecte les interactions avec des sources connues, comme les serveurs liés aux stalkerwares. TinyCheck peut également être utilisé pour vérifier n'importe quel appareil sur n'importe quelle plateforme, y compris iOS, Android, ou tout autre système d'exploitation.

Vous pensez être victime d›un stalkerware ? Voici quelques conseils…

Que vous soyez ou non victime de stalkerware, voici quelques conseils pour mieux vous protéger :

- Protégez votre téléphone avec un mot de passe fort que vous ne partagez jamais avec votre partenaire, vos amis ou vos collègues.
- Modifiez périodiquement les mots de passe de tous vos comptes et ne les partagez avec personne.
- Ne téléchargez que des applications provenant de sources officielles, comme Google Play ou l'App Store d'Apple.
- Installez une solution de sécurité informatique fiable comme Kaspersky for Android sur les appareils et procédez à leur analyse régulière. Cependant, si un stalkerware est déjà installé, cette opération ne doit être effectuée qu'après avoir évalué le risque pour la victime, car l'agresseur peut remarquer l'utilisation d'une solution de cybersécurité.

Les victimes de stalkerware peuvent être victimes d'un cycle plus vaste d'abus, notamment physiques.

Dans certains cas, l'agresseur est averti si sa victime effectue une analyse de l'appareil ou supprime une application de stalkerware. Une telle situation pourrait aggraver le problème et entraîner de nouvelles formes d'agression. C'est pourquoi il est important de procéder avec prudence si vous pensez être la cible d'un stalkerware.

- **Contactez une organisation de soutien locale :** pour en trouver une près de chez vous, consultez le site de la Coalition Against Stalkerware.
- **Soyez attentif aux avertissements suivants :** il se peut que votre batterie se décharge rapidement à cause d'applications inconnues ou suspectes gourmandes en ressources, et que des applications nouvellement installées avec un accès suspect permettent d'utiliser et de suivre votre localisation, d'envoyer ou de recevoir des messages texte et de surveiller d'autres activités personnelles. Vérifiez également si le paramètre « sources inconnues » est activé sur votre appareil. Si c'est le cas, il se peut qu'un logiciel indésirable ait été installé à partir d'une source tierce. Cependant, les indicateurs ci-dessus sont des indices et n'indiquent pas la présence sans équivoque d'un stalkerware sur l'appareil.
- **N'essayez pas d'effacer le stalkerware ni de modifier les paramètres de votre téléphone :** vous risquez d'alerter votre agresseur potentiel et d'aggraver la situation. Vous risquez également d'effacer des données ou des preuves importantes qui pourraient être utilisées dans le cadre d'une poursuite judiciaire.

Pour en savoir plus à propos de nos activités relatives aux stalkerwares ou pour toute autre demande, veuillez nous contacter par écrit à l'adresse suivante : 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/

TinyCheck:
https://tiny-check.com

Coalition Against Stalkerware

TinyCheck®

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