L'état des **stalkerware** en 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST
STALKERWARE

À propos de la Coalition contre les stalkerware

Ce nouveau groupe de travail mondial vise à combiner le savoir-faire d'entreprises du domaine de la cybersécurité et l'expertise d'organisations de lutte contre les violences domestiques afin d'aider les victimes de stalkerwares, ou logiciels « espions » ou encore « de traque »

En novembre 2019, dix organisations – Avira, l'Electronic Frontier Foundation, le Réseau européen pour le travail avec les auteurs de violences conjugales (WWP EN), DATA CyberDefense, Kaspersky, Malwarebytes, le Réseau national de lutte contre les violences conjugales (NNEDV), NortonLifeLock, Operation: Safe Escape et WEISSER RING – lançaient une initiative mondiale appelée « Coalition contre les stalkerware » et visant à protéger le public de ces logiciels.

L'idée première derrière la formation de cette Coalition est de faciliter la communication entre les acteurs du domaine de la cybersécurité et les organisations de lutte contre les violences conjugales. Grâce à son portail en ligne, www.stopstalkerware.org, la Coalition se donne également pour objectif d'aider les victimes, de faciliter le partage de connaissances entre ses membres, de développer une série de bonnes pratiques en matière de développement de logiciels éthiques et d'informer le public des dangers des stalkerwares.

Ce projet a été imaginé comme une initiative non commerciale visant à réunir autour d'une même table des intervenants issus d'organisations à but non lucratif, d'entreprises de la cybersécurité, mais aussi d'autres domaines clés à l'instar des autorités judiciaires. En raison de son importance sociétale majeure pour les utilisateurs du monde entier et des nouvelles formes de stalkerwares régulièrement développées, la Coalition contre les stalkerware est ouverte à de nouveaux partenaires et appelle à une coopération toujours plus élargie.

Pour plus d'informations, rendez-vous sur www.stopstalkerware.org

Témoignages des membres fondateurs de la Coalition sur la collaboration contre les stalkerwares :

Alexander Vukcevic,
Directeur de Protection Labs,
Avira

« Les logiciels de contrôle ont énormément évolué ces dernières années. De puissantes fonctions de surveillance ont ainsi vu le jour et les finalités des activités de suivi ont fondamentalement changé. L'explosion de l'utilisation des appareils mobiles, combinée à l'absence de cadre législatif, permet aujourd'hui à quiconque d'accéder en toute simplicité à des outils permettant d'espionner conjoints, membres de sa famille ou encore amis. Avira reconnaît qu'il s'agit d'une nouvelle catégorie de menaces et invite les entreprises du domaine de la sécurité informatique et les organisations luttant contre les violences conjugales à unir leurs forces, à échanger leurs informations et à coopérer pour mettre un terme à ces violations de la vie privée. »

Eva Galperin,
Directrice de la cybersécurité,
Electronic Frontier Foundation

« Les stalkerwares utilisés pour espionner les téléphones et les ordinateurs dans les cas de violence conjugale ou de harcèlement, constituent un problème très grave, allant souvent de pair avec d'autres formes de violence, y compris celle physique. L'omniprésence des stalkerwares est un problème complexe et nous avons besoin d'acteurs issus de tous les secteurs pour les combattre efficacement. »

Anna McKenzie, Responsable de la communication, **Réseau européen pour le travail avec les auteurs de violences conjugales (WWP EN)**

« Des études ont démontré que 70 % des femmes victimes de cyberharcèlement avaient également subi au moins une forme de violence physique et/ou sexuelle de la part de leurs partenaires intimes. Nous devons empêcher les auteurs de ces violences d'utiliser le téléphone de leurs partenaires pour les traquer, et nous devons également les tenir responsables de leurs actes. La Coalition contre les stalkerware nous permet de transmettre nos connaissances en matière de violences basées sur le genre et leurs auteurs aux entreprises du domaine de la sécurité informatique, et ce afin de collaborer pour mettre un terme aux violences envers les femmes de tout âge perpétrées au moyen des nouvelles technologies. »

Hauke Gierow,
Porte-parole,
G DATA CyberDefense

« Le fait de placer des logiciels espions sur le téléphone de son ou sa partenaire constitue une violation des droits fondamentaux de l'homme. Nous sommes déterminés à lutter contre cette pratique et à protéger les victimes de ces abus, principalement des femmes. G DATA CyberDefense s'engage à mieux sensibiliser ses utilisateurs aux risques potentiels et à collaborer avec les organisations d'aide aux victimes afin de s'attaquer également aux problèmes non techniques liés aux stalkerwares. »

Vyacheslav Zakorzhevsky,
Responsable de la recherche anti-malware, Kaspersky

« Afin de remédier à ce problème, il est important que les entreprises du domaine de la cybersécurité et les organisations de lutte contre les violences domestiques unissent leurs forces. Le secteur de la sécurité informatique contribue en améliorant la détection des stalkerwares et en sensibilisant davantage ses utilisateurs sur cette menace pour leur vie privée. En parallèle, les organisations de soutien et de défense des droits des victimes de violences conjugales collaborent directement avec ces dernières, identifiant leurs difficultés et attentes afin de mieux guider notre travail. En travaillant de concert, nous pourrons renforcer notre expertise technique et nos capacités afin de mieux accompagner les victimes. »

David Ruiz,
Rédacteur spécialisé dans la confidentialité en ligne,
Malwarebytes Labs

« Depuis des années, Malwarebytes détecte et avertit les utilisateurs des fonctionnalités potentiellement dangereuses des stalkerwares, une menace invasive capable de priver les individus de leurs attentes et de leurs droits en matière de confidentialité. Tout comme les abus qu'ils peuvent occasionner, les stalkerwares prolifèrent également hors de la vue du public, laissant leurs victimes démunies et isolées. La formation de la Coalition contre les stalkerware et la collaboration au sein de ce groupe de travail constituent la prochaine étape indispensable pour mettre fin à cette menace numérique. Elle s'impose ainsi comme une approche collaborative, axée sur la promesse de permettre l'utilisation des nouvelles technologies de manière sécurité, pour tous et partout. »

Erica Olsen,
Directrice du projet Safety Net,
Réseau national de lutte contre les violences conjugales (NNEDV)

« Lorsqu'ils sont utilisés de manière discrète, ne générant ainsi aucune notification, les stalkerwares peuvent s'imposer comme de puissants outils pour perpétrer diverses formes d'abus, du harcèlement à la surveillance en passant par la fraude ou encore la traque. Ces agissements peuvent être terrifiants, traumatisants et susciter de vives inquiétudes en matière de sécurité et de respect de la vie privée. La formation de cette Coalition est un pas en avant majeur dans la lutte contre ce problème. »

Kevin Roundy,
Directeur de la recherche,
NortonLifeLock

« Chez NortonLifeLock, nos experts en recherche s'efforcent depuis plus de 12 ans d'empêcher les personnes malintentionnées de se procurer des stalkerwares, offrant ainsi aux victimes avérées et potentielles les outils nécessaires pour se protéger face aux différentes formes de harcèlement, violence et attaques. Nous sommes fiers de compter parmi les membres fondateurs de la Coalition Against Stalkerware afin de partager notre expertise et d'unir nos forces dans la lutte contre ce fléau. »

Wilson « Chilly » Hightower,
Responsable de l'accueil,
Operation: Safe Escape

« L'existence insidieuse de stalkerwares ne sert qu'à nuire, blesser et insuffler un sentiment constant de peur et d'anxiété chez bon nombre des personnes que nous accompagnons. C'est une menace constante et existentielle pour la sécurité et la vie privée de tous. Alors que nos vies sont de plus en plus dépendantes des technologies, la menace des stalkerwares ne cesse de prendre de l'ampleur. Il est ainsi plus important que jamais de prendre les devants face à cette menace afin de priver de potentiels auteurs de harcèlement et autres formes de violence d'un accès à ces outils. Operation: Safe Escape est très fier de participer à cet effort collectif visant à rétablir la confidentialité et à offrir un sentiment de sécurité chez les personnes que nous accompagnons, mais aussi chez l'ensemble des utilisateurs des nouvelles technologies. »

Horst Hinger,
Directeur général adjoint,
WEISSER RING

« En tant qu'organisation à but non lucratif, nous savons que les technologies permettent à des personnes malveillantes d'accéder plus facilement aux données privées de leurs victimes. En outre, les victimes demandent rarement de l'aide en raison d'un sentiment de honte. Pour WEISSER RING, le harcèlement constitue un problème de plus en plus important dans le cadre de notre accompagnement des victimes. En 2018, nous avons accompagné 1 019 cas de cyberharcèlement, soit 3 % de plus que l'année précédente. D'autre part, selon les statistiques de la police allemande, il y aurait eu en 2018 près de 19 000 cas de cyberharcèlement, soit 500 de plus que l'année précédente, ce qui représente également une nette augmentation. C'est pourquoi nous avons développé l'application NO STALK en collaboration avec la fondation WEISSER RING afin de fournir aux victimes de harcèlement un outil efficace pour en conserver les preuves matérielles. »

Conclusions principales, mises à jour en avril 2020

Dans le monde entier, le nombre d'utilisateurs dont les appareils abritent des stalkerwares a augmenté de 67 % en un an seulement

Cette section fournit une mise à jour des chiffres pour l'année complète 2019 par rapport à l'année 2018. En raison de la date de publication, la partie restante du rapport contient les données de janvier à août 2019.

- À la fin de l'année 2019, le nombre de nos utilisateurs d'appareils mobiles victimes de stalkerwares a augmenté de 67%: 40,386 utilisateurs uniques ont été attaqués en 2018, tandis qu'en 2019, ce nombre est passé à 67,500
- Le nombre de ces attaques a doublé au cours du second semestre 2019 par rapport au premier semestre. En janvier 2019, 4 483 utilisateurs d'appareils mobiles de Kaspersky ont été attaqués; en septembre 2019, ce nombre est passé à 9,546, et, en décembre 2019, le nombre d'utilisateurs touchés a atteint 11,052
- Dans le monde entier, la Russie, le Brésil, l'Inde et les États-Unis sont les pays les plus touchés par les stalkerwares, représentant respectivement 23.4%, 9.4%, 9% et 5.6% des utilisateurs concernés en 2019
- En ce qui concerne l'Europe, l'Allemagne (3.1%), l'Italie (2.4%) et la France (1.8%) occupent respectivement les trois premières places

Introduction et méthodologie

Il y a six mois, nous avons créé une alerte spéciale qui informe les utilisateurs des logiciels espions commerciaux (stalkerware) installés sur leurs téléphones. Ce rapport examine l'utilisation des stalkerware et le nombre d'utilisateurs touchés par ces logiciels au cours des huit premiers mois de l'année 2019.

La technologie de surveillance des consommateurs a évolué rapidement au cours des dernières années et le but même de l'activité de surveillance a changé radicalement. L'essor d'Internet et l'explosion de l'utilisation des appareils mobiles qui s'en est suivie ont donné naissance à un type de logiciel de surveillance florissant, connu sous le nom de stalkerware. Le logiciel permet aux utilisateurs d'espionner d'autres personnes (par exemple, pour surveiller leurs messages, leurs informations d'appel et leur emplacement GPS) en toute discrétion. Il peut souvent être utilisé pour abuser de la vie privée d'anciens partenaires ou d'un partenaire actuel et même de celle de personnes inconnues. Pour ce faire, il suffit d'installer manuellement une application sur le smartphone ou la tablette de la victime ciblée. Une fois en place, l'espion a accès à toute une gamme de données personnelles, tout en étant loin de la victime. Ce logiciel diffère grandement des logiciels de contrôle parental. Alors que les applications de contrôle parental visent à restreindre l'accès au contenu risqué et inapproprié et à informer constamment un utilisateur à propos de ses requêtes, le stalkerware permet à l'agresseur de surveiller et d'espionner une victime, sans le consentement d'une personne.

Le stalkerware permet à l'agresseur de surveiller et d'espionner une victime, sans le consentement d'une personne

La grande majorité des applications stalkerware ne sont pas disponibles dans les boutiques d'applications officielles, comme Google Play, et l'installation nécessite l'accès à un site Web dédié et à l'appareil de la victime. Les personnes avec de mauvaises intentions peuvent les utiliser pour surveiller les e-mails des employés, pour suivre les déplacements des enfants et même pur espionner les activités d'un partenaire. De telles utilisations peuvent mener à l'intimidation, à la surveillance sans consentement, au harcèlement et même à la violence familiale. Toutefois, les lois actuelles visant à réglementer l'utilisation des stalkerware ne sont pas encore assez strictes pour dissuader les coupables d'abuser et de profiter d'autres personnes.

Les données de ce rapport ont été tirées de statistiques agrégées sur les menaces obtenues de Kaspersky Security Network, afin de mesurer la fréquence et le nombre d'utilisateurs qui ont été confrontés à des menaces de stalkerware au cours des huit premiers mois de l'année 2019, et de comparer ces données à ce qui a été constaté l'année dernière. Le Kaspersky Security Network est l'infrastructure dédiée au traitement des flux de données liées à la cybersécurité provenant de millions de participants bénévoles dans le monde entier. Dans ce blog, nous avons cherché à savoir pourquoi les stalkerware sont utilisés et où ceux-ci sont le plus souvent implémentés.

Résultats principaux

Au niveau mondial, on constate une augmentation de 35% du nombre d'utilisateurs confrontés au moins une fois à un stalkerware

- De janvier à août 2019, dans le monde entier, plus de 518 223 cas ont été recensés lorsque nos technologies de protection ont soit enregistré la présence de stalkerware sur les appareils des utilisateurs, soit détecté une tentative d'installation d'un stalkerware : une augmentation de 373 % durant la même période en 2018

- Au cours des huit premiers mois de 2019, 37 532 utilisateurs ont été confrontés au moins une fois à un stalkerware. Il s'agit d'une augmentation de 35 % par rapport à la même période en 2018 où 27 798 utilisateurs ont été ciblés

- Le nombre d'utilisateurs ciblés par les logiciels espions à plein régime détectés comme étant des chevaux de Troie espions a atteint 26 620 au cours des huit premiers mois de l'année 2019, soit une minorité si l'on compare le nombre d'utilisateurs qui ont été confrontés aux stalkerware

- La Fédération de Russie reste la région la plus touchée par les stalkerware dans le monde, représentant 25,6 % des utilisateurs potentiellement concernés au cours des huit premiers mois de l'année 2019. L'Inde arrive en deuxième position avec 10,6 % des utilisateurs concernés et le Brésil en troisième position (10,4 %). Les États-Unis occupent la quatrième place avec 7,1 %.

- En Europe, l'Allemagne, l'Italie et le Royaume-Uni occupent respectivement les trois premières places.

Le problème des stalkerware en hausse

Cette année a connu une forte augmentation du nombre de détections de stalkerware sur les appareils Android protégés par des produits Kaspersky. L'une des raisons de cette augmentation pourrait être l'amélioration de la détection des stalkerware grâce à des solutions de cybersécurité. En avril, Kaspersky a lancé une fonctionnalité dans son application de sécurité Android : Privacy Alert. Cette fonctionnalité alerte de manière spécifique les utilisateurs si un logiciel pouvant être utilisé pour l'espionnage est identifié sur leur appareil. Depuis lors, le nombre de détections n'a cessé d'augmenter. Par exemple, 4 315 utilisateurs ont été confrontés aux stalkerware en mars 2019, par rapport à 7 075 en avril – une augmentation de 64 % en seulement un mois. Ce nombre est passé à 9 251 en août, soit 94 % de plus que le mois précédant le lancement de la fonctionnalité.

Ces programmes de surveillance des consommateurs vendus ouvertement sont souvent utilisés pour espionner des collègues, des membres de la famille ou des partenaires, et ceux-ci sont en demande constante. Moyennant des coûts relativement modestes, parfois aussi peu que 7 € par mois, ces applications restent cachées tout en tenant leurs opérateurs informés de l'activité de l'appareil, comme l'emplacement du propriétaire, l'historique du navigateur, les SMS, les discussions sur les médias sociaux, et bien plus. Certains d'entre eux peuvent même effectuer des enregistrements vidéo et vocaux.

Pour examiner plus en détail l'étendue du problème des stalkerware, Kaspersky a analysé l'activité au cours des huit derniers mois. Entre janvier et août 2019, 37 533 utilisateurs ont été confrontés à des stalkerware sur leurs appareils au moins une fois. Il s'agit d'une augmentation de 35 % par rapport à la même période en 2018 où 27 798 utilisateurs ont été ciblés. Dans l'ensemble, 518 223 cas ont été recensés lorsque les produits Kaspersky ont soit enregistré la présence d'un stalkerware sur les appareils des utilisateurs, soit détecté une tentative d'installation entre janvier et août 2019 : une augmentation stupéfiante de 373 % par rapport à la même période en 2018.

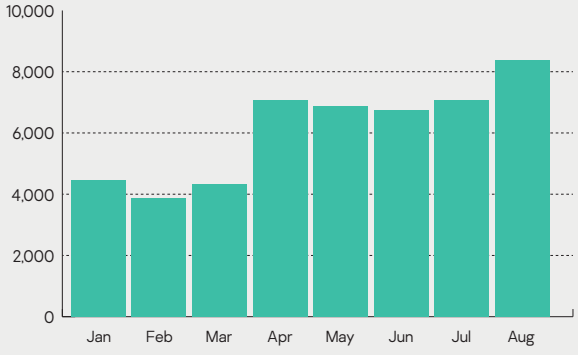


Fig.1 Nombre d'utilisateurs qui ont été confrontés aux stalkerware en janvier-août 2019

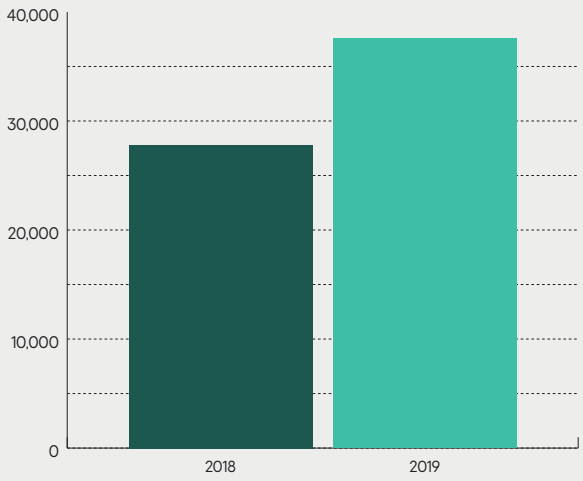
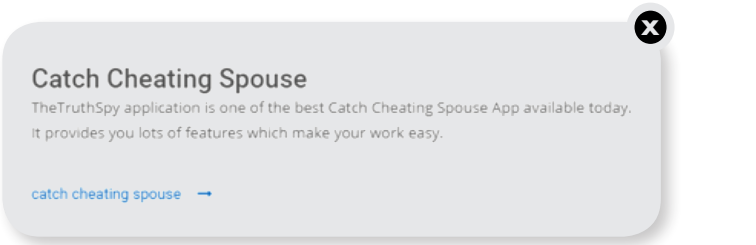


Fig.2 Utilisateurs ciblés par les stalkerware 2018 contre 2019



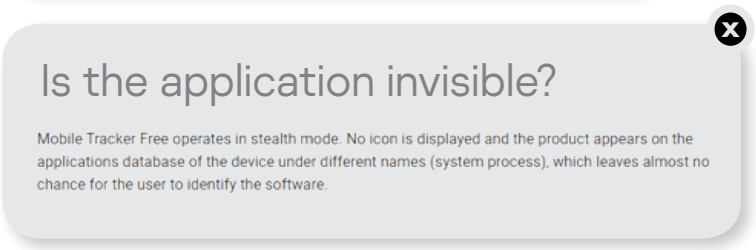


Fig.3 Captures d'écran du site officiel de Mobile Tracker Free

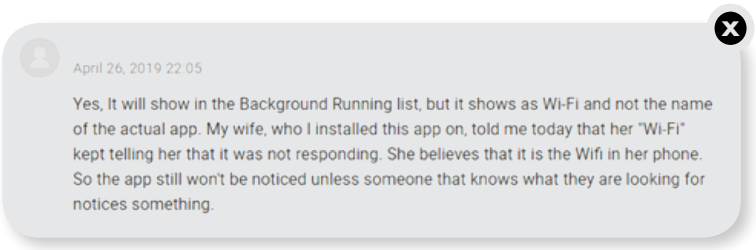


Fig.4 Capture d'écran du site officiel de TheTruthSpy

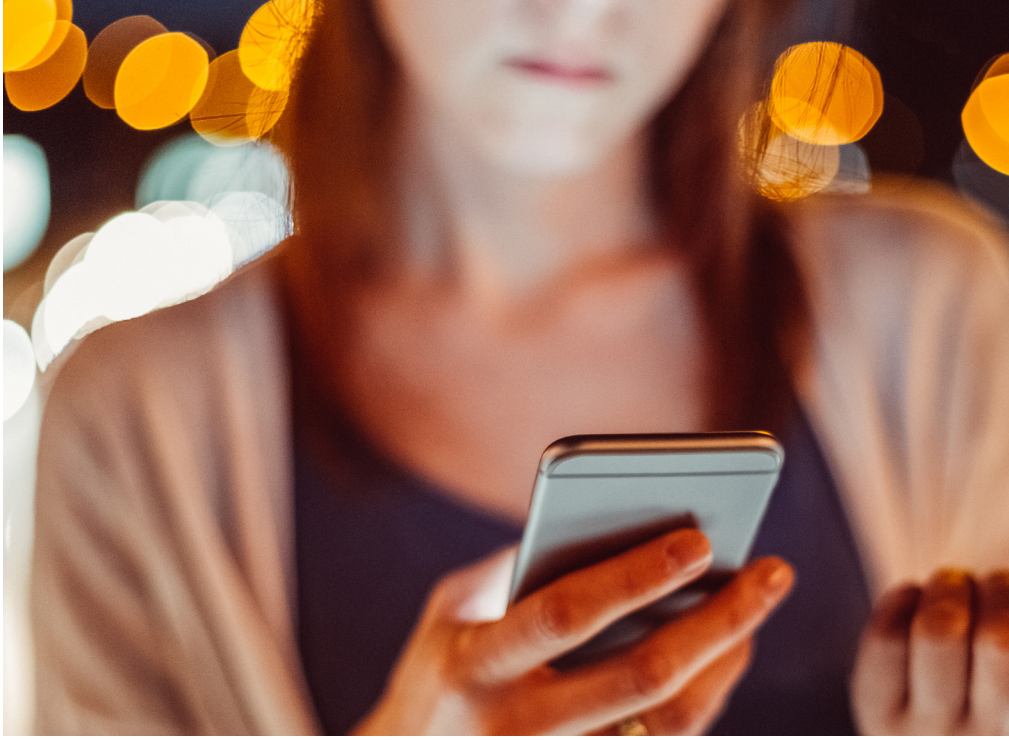
Exemples de logiciels utilisés à des fins d'espionnag

Un tiers peut également accéder en temps réel aux photos des victimes à partir du téléphone et de l'appareil photo, ainsi qu'à l'historique de leur navigateur, aux fichiers de l'appareil, au calendrier et à la liste des contacts

La famille des stalkerware la plus répandue en 2019 a été identifiée sous le nom de Monitor.AndroidOS.MobileTracker.a et a touché 6 559 utilisateurs uniques. En deuxième position, Monitor.AndroidOS.Cerberus.a a été détecté sur les appareils de 4 370 utilisateurs, suivi de près en troisième position par Monitor.AndroidOS.Nidb.a (4 047).

Si l'on compare les résultats de 2018, les deux premiers diffèrent de ceux de l'an dernier. Monitor.AndroidOS.Nidb.a et Monitor.AndroidOS.PhoneSpy.b se retrouvaient le plus sur les appareils des utilisateurs en 2018, atteignant 4 427 et 2 819 utilisateurs respectivement. Monitor.AndroidOS.XoloSale.a était le troisième stalkerware le plus répandu atteignant 1 946 utilisateurs.

Dans notre système de classification interne, un enregistrement Monitor.AndroidOS.MobileTracker.a est utilisé pour identifier une application Mobile Tracker Free, qui se positionne comme un outil permettant de suivre l'activité des enfants ou des employés. En effet, l'application permet de suivre l'emplacement de l'utilisateur, ses correspondances aussi bien dans les SMS que dans les applications de messagerie (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, etc.), ainsi que ses appels. Un tiers peut également accéder en temps réel aux photos des victimes à partir du téléphone et de l'appareil photo, ainsi qu'à l'historique de leur navigateur, aux fichiers de l'appareil, au calendrier et à la liste des contacts. De plus, l'application offre la possibilité de contrôler l'appareil à distance. En plus de tout cela, il est possible de travailler dans un mode caché en utilisant les applications système comme camouflage.



Où trouve-t-on des stalkerware ?

Il existe un marché mondial pour les logiciels espions et les stalkerware légaux, comme le prouve la diversité des régions où se produisent la plupart des attaques. Les 10 premiers pays qui comptent le plus grand nombre d'utilisateurs victimes de stalkerware ne présentent pas de similitudes géopolitiques et ne sont pas très proches les uns des autres.

1. Russian Federation – **25.61%**
2. India – **10.56%**
3. Brazil – **10.39%**
4. United States – **7.11%**
5. Germany – **3.55%**
6. Italy – **2.65%**
7. Mexico – **2.10%**
8. United Kingdom – **1.95%**
9. France – **1.76%**
10. Iran – **1.68%**

Other – **32.65%**

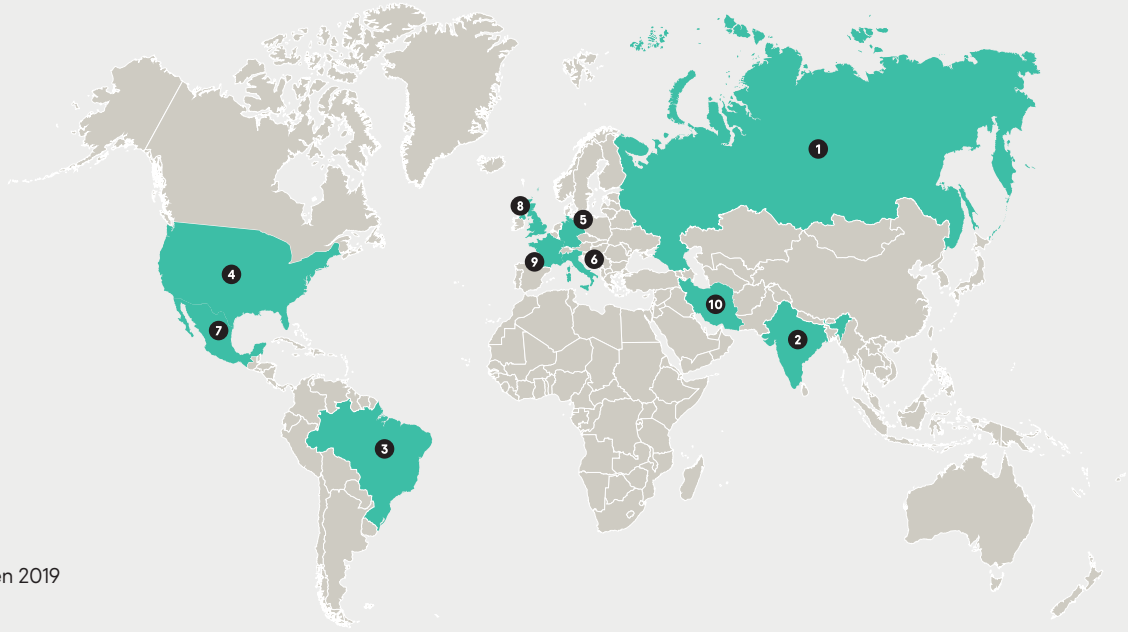


Fig. 5 Géographie des utilisateurs qui ont été confrontés aux stalkerware en 2019

85 % des intervenants dans les cas de violence familiale ont dit avoir aidé des victimes dont l'agresseur les avait suivis au moyen d'un GPS

Les résultats de Kaspersky montrent que la Russie est la région où l'activité des stalkerware est la plus intense. Les activités continues en Inde ont fait du pays la deuxième région la plus touchée par des incidents liés aux stalkerware de janvier à août, avec 10,56 % des utilisateurs concernés.

Le Brésil comptait 10,39 % des utilisateurs attaqués en 2019, tandis que les États-Unis occupent désormais le quatrième rang (7,11 %). Des groupes de défense des droits sont présents dans le pays pour sensibiliser la population aux dangers des stalkerware et mener des recherches révélatrices sur les utilisateurs. 72 refuges pour victimes de violence familiale ont été interrogés par la Radio publique nationale, et 85 % des intervenants dans les cas de violence familiale ont dit avoir aidé des victimes dont l'agresseur les avait suivis au moyen d'un GPS. Près de trois quarts (71 %) des auteurs de violence familiale surveillent les activités informatiques des survivants, tandis que 54 % d'entre eux suivent les appels téléphoniques cellulaires des survivants au moyen d'un stalkerware. Le cinquième pays le plus touché en 2019 était l'Allemagne avec (3,55 %).

Les stalkerware dans le contexte de la cybermenace

En 2019, plus de 37 000 personnes ont été confrontées à un stalkerware, contre à peine 27 000 l'année précédente

Lorsque l'on compare les stalkerware et les logiciels espions au reste des attaques auxquelles sont confrontés les utilisateurs de téléphones mobiles, comme les logiciels publicitaires, les logiciels à risques et les programmes malveillants, on constate qu'ils englobent une grande part des applications non-virus moins ciblées. Au cours des huit premiers mois de l'année 2019, Kaspersky a détecté 2 350 862 utilisateurs victimes de menaces potentiellement indésirables et seulement 1,60 % d'entre eux étaient touchés par des stalkerware. Cependant, contrairement à la majorité des menaces potentielles de masse (comme les logiciels publicitaires), les stalkerware ont besoin d'un espion spécifique pour agir et mener à bien son opération. Chaque cible est traquée et sélectionnée intentionnellement. Ainsi, bien que les statistiques soient plus faibles, les stalkerware exigent un effort plus ciblé pour toucher une victime et, derrière chacun de ces nombres, se cache une forme d'abus inquiétante.

Pour avoir une vue d'ensemble lors de l'évaluation de la dynamique de développement des stalkerware, nous avons comparé les stalkerware aux programmes malveillants de surveillance illégale à grande échelle pour PC que nous identifions comme chevaux de Troie espions. Les résultats ont démontré que si les logiciels espions illégaux sont en déclin, les stalkerware sont en plein essor.

Notre analyse des huit premiers mois de 2019 montre que le nombre d'utilisateurs qui ont été confrontés aux stalkerware a, en fait, dépassé le nombre d'attaques de chevaux de Troie espions. Alors que l'année 2018 a connu plus de 43 000 cibles de logiciels espions contre 28 000 cibles de stalkerware, en 2019 la situation a changé. Le nombre d'utilisateurs qui ont été confrontés aux stalkerware a augmenté de 35 % pour atteindre plus de 37 000 personnes, tandis que les outils logiciels espions représentaient 26 620 cibles.

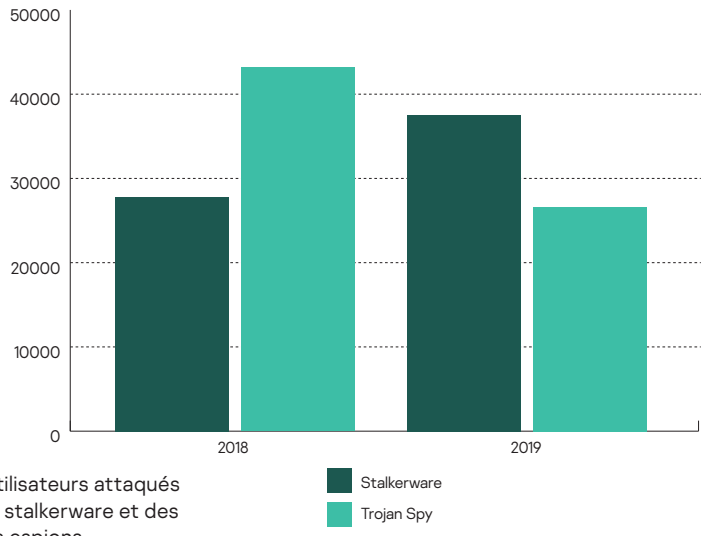


Fig. 6 Utilisateurs attaqués par des stalkerware et des logiciels espions

Le nombre d'incidents liés aux stalkerware enregistrés par les produits Kaspersky a connu une augmentation notable par rapport à l'ensemble des menaces en 2018, selon les statistiques de cette année. Entre janvier et août de l'année dernière, ces logiciels ne représentaient que 1,01 % du nombre total d'utilisateurs confrontés à tout type de logiciel potentiellement dangereux (logiciels publicitaires et autres de la catégorie des logiciels non-virus) (2 740 023). Les stalkerware semblent gagner en popularité, tandis que les attaques de programmes malveillants plus traditionnelles sont moins répandues qu'il y a 12 mois.

Conclusion et recommandations

Il est clair que les stalkerware sont en pleine expansion et qu'ils occupent une place de plus en plus importante dans le contexte de la cybersécurité. Conformément au nombre total de fluctuations d'une année à l'autre du nombre d'attaques détectées de logiciels à risques, de logiciels publicitaires et de logiciels espions, le taux d'incidents liés aux stalkerware ne cesse de grimper. Il faudra peut-être du temps pour découvrir le rôle des espions dans le contexte de la cybermenace, mais d'autres incidents sont dorénavant pris en compte. Grâce à l'amélioration des logiciels de cybersécurité, on observe une forte augmentation depuis que Kaspersky a lancé sa propre solution pour informer les utilisateurs des stalkerware en avril 2019.

On constate également un certain degré de cohérence quant aux pays les plus susceptibles d'être victimes d'incidents liés aux stalkerware, la Russie, l'Inde, les États-Unis et l'Allemagne étant parmi les plus touchés au cours des deux dernières années.

Heureusement pour les utilisateurs, des fonctionnalités et des solutions efficaces sont mises en place pour leur permettre de se protéger. Des solutions pratiques pour résoudre le problème sont en train de faire leur apparition. Les entreprises de sécurité informatique et les organisations de défense des droits qui travaillent avec les victimes de violence familiale devraient unir leurs forces pour veiller à ce que les entreprises de cybersécurité réagissent mieux aux stalkerware. De telles initiatives aideraient les victimes grâce à la technologie et à l'expertise.

Nous croyons que chaque personne a droit à la protection de sa vie privée. C'est pourquoi nous proposons notre expertise en matière de sécurité, travaillons en étroite collaboration avec des organisations internationales et des organismes d'application de la loi pour lutter contre les cybercriminels, et développons des technologies, des solutions et des services qui vous aident à vous prémunir des cybermenaces.

À propos de Kaspersky

« Kaspersky est une société de cybersécurité mondiale fondée en 1997. L'expertise de Kaspersky en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky aident plus de 400 millions d'utilisateurs et 270 000 entreprises à protéger ce qui compte le plus pour eux. Pour en savoir plus : www.kaspersky.fr. «

www.kaspersky.com

www.securelist.com

kaspersky