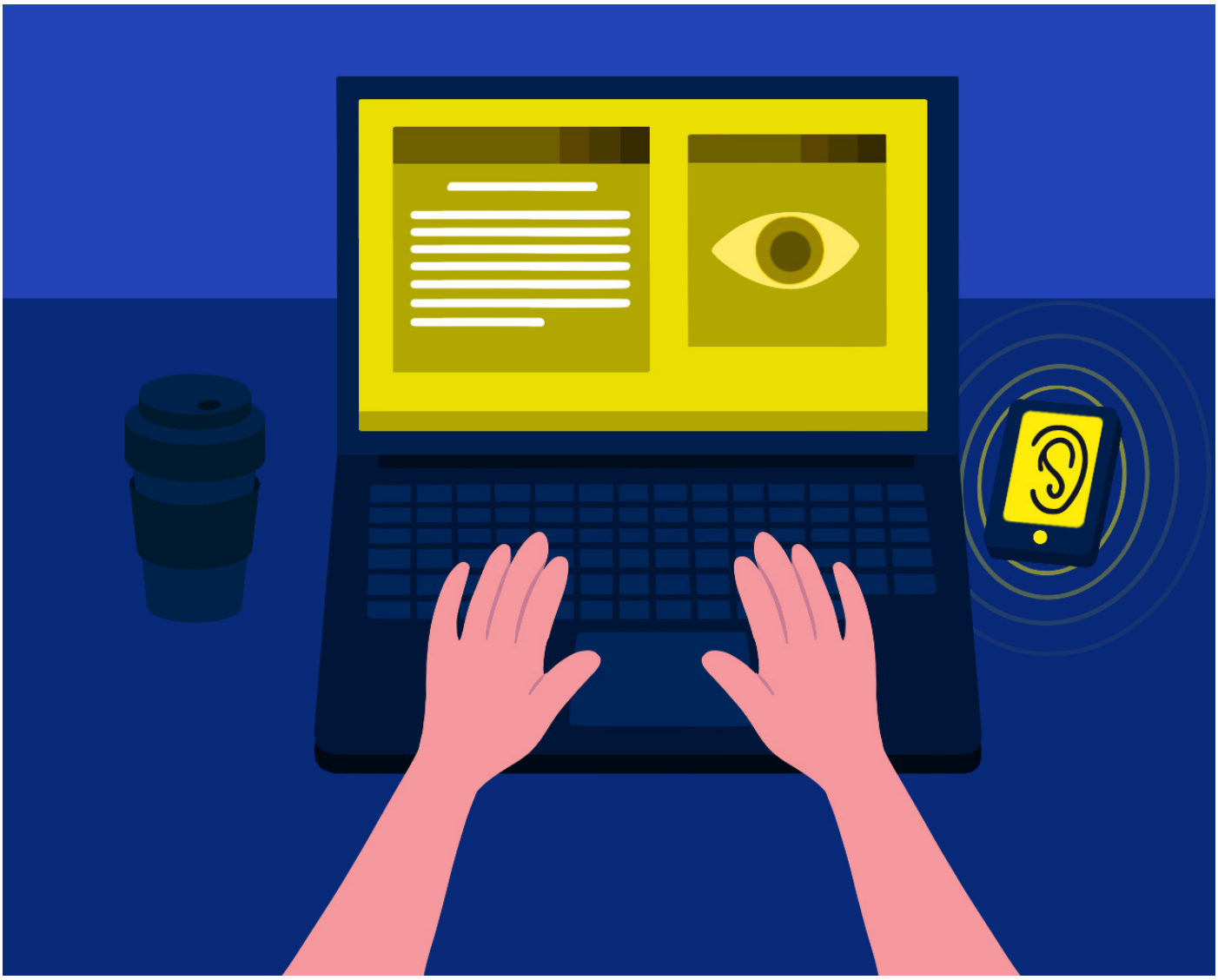


O estado do **Stalkerware** em 2021

COALITION AGAINST STALKERWARE

kaspersky

Conteúdo

Principais resultados de 2021

Todos os anos, a Kaspersky analisa o uso de stalkerware em todo o mundo para entender melhor a ameaça que ele representa. Estabelecemos parcerias com partes interessadas nos setores público e privado para aumentar a conscientização e encontrar soluções para lidar melhor com esse importante problema.

O stalkerware permite que as pessoas espionem secretamente a vida privada de outras pessoas através de dispositivos inteligentes e é frequentemente usado para facilitar a violência psicológica e física contra parceiros íntimos. O software está disponível comercialmente e pode acessar uma variedade de dados pessoais, incluindo localização do dispositivo, histórico do navegador, mensagens de texto, bate-papos em redes sociais, fotos e muito mais. A comercialização de stalkerware não é ilegal, mas sua utilização sem o consentimento da vítima sim. Os agressores se beneficiam desse enquadramento legal vago que ainda existe em muitos países. Stalkerware é uma violação de privacidade e uma forma de abuso de tecnologia. Para enfrentar essa ameaça complexa de uma forma abrangente que apoie as vítimas e sobreviventes de uma melhor forma, são necessárias ferramentas inovadoras do ponto de vista legislativo, social e tecnológico.

Destaques de dados de 2021

- **Em 2021, os dados da Kaspersky mostram que 32.694 usuários únicos foram afetados por stalkerware em todo o mundo.** Isso representa uma diminuição em relação aos nossos números de 2020 e uma baixa histórica desde que começamos a coletar dados sobre stalkerware em 2018. Embora isso possa ser visto como um motivo de comemoração, não é.
- **A violência cibernética está em ascensão,** especialmente desde o início da pandemia. À medida que as pessoas continuam a socializar menos e a passar mais tempo em casa, os agressores se sentem mais no controle, possivelmente tornando-os menos propensos a instalar stalkerware para espionar seu parceiro. Além disso, os agressores, infelizmente, têm uma gama mais ampla de meios, na forma de dispositivos inteligentes, para espionar ou perseguir suas vítimas. Organizações sem fins lucrativos com as quais a Kaspersky trabalha de perto compartilharam observações semelhantes ao trabalhar com agressores e vítimas de stalkerware. É importante lembrar que esses números incluem apenas usuários da Kaspersky: eles não levam em consideração os usuários das soluções de segurança de TI dos nossos concorrentes ou aqueles que não possuem nenhuma solução de segurança de TI instalada em seus celulares. Portanto, vemos apenas a ponta do iceberg: embora seja difícil calcular o número exato de usuários afetados no mundo, membros da Coalition Against Stalkerware estimam que pode ser pelo menos 30 vezes maior, com cerca de um milhão de vítimas globalmente a cada ano.

- Com base em dados obtidos da Kaspersky Security Network, **os países mais afetados continuam sendo Rússia, Brasil e Estados Unidos.** Isso está de acordo com as estatísticas dos últimos dois anos. No nível regional, encontramos o maior número de usuários afetados nos seguintes países:
- Alemanha, Itália e Reino Unido (Europa)
- Turquia, Egito e Arábia Saudita (Oriente Médio e África)
- Índia, Indonésia e Vietnã (Ásia-Pacífico)
- Brasil, México e Colômbia (América Latina)
- Estados Unidos (América do Norte)
- Federação Russa, Ucrânia e Cazaquistão (Europa Oriental (exceto países da UE), Rússia e Ásia Central)
- **Cerberus e Reptilicus foram os aplicativos de stalkerware mais usados,** com 5.575 e 4.417 usuários afetados, respectivamente, em todo o mundo.

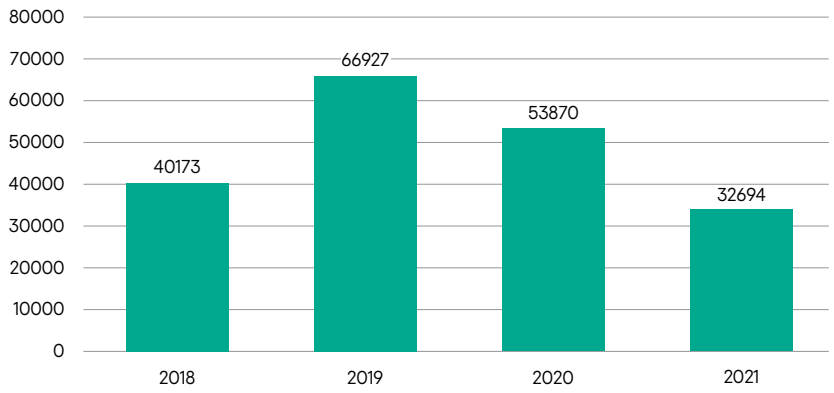
Tendências observadas pela Kaspersky

Números globais de detecção: usuários afetados

Nesta seção, destacamos os números globais e regionais observados pela Kaspersky em 2021 e como eles se comparam aos de anos anteriores.

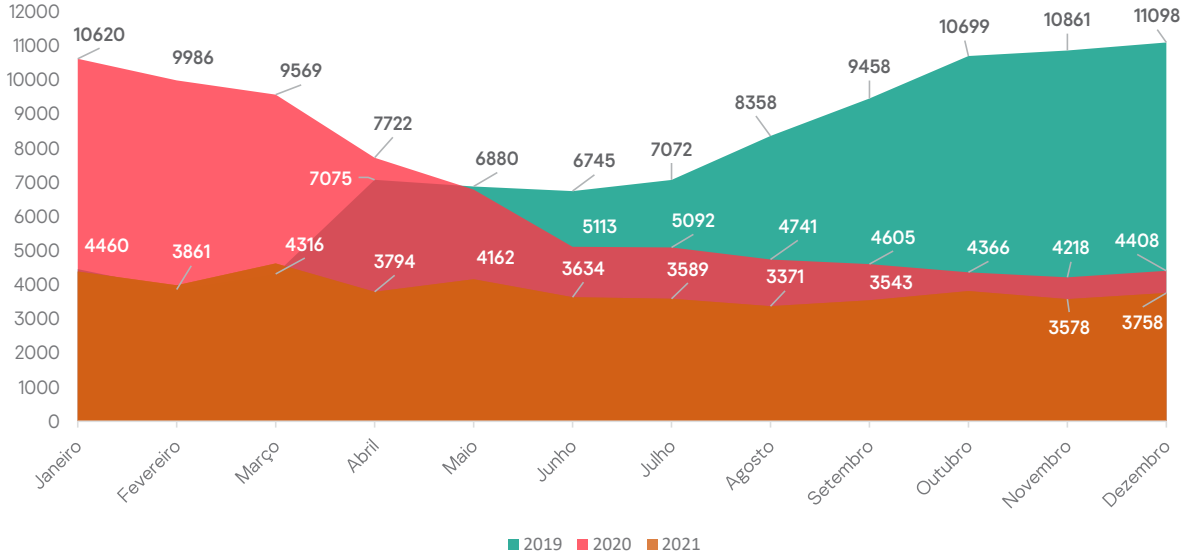
Em 2021, um total de 32.694 usuários únicos foram afetados por stalkerware

Em 2021, um total de 32.694 usuários únicos foram afetados por stalkerware. O gráfico abaixo mostra a evolução dos usuários afetados ano a ano desde 2018.



Evolução dos usuários afetados ano a ano desde 2018

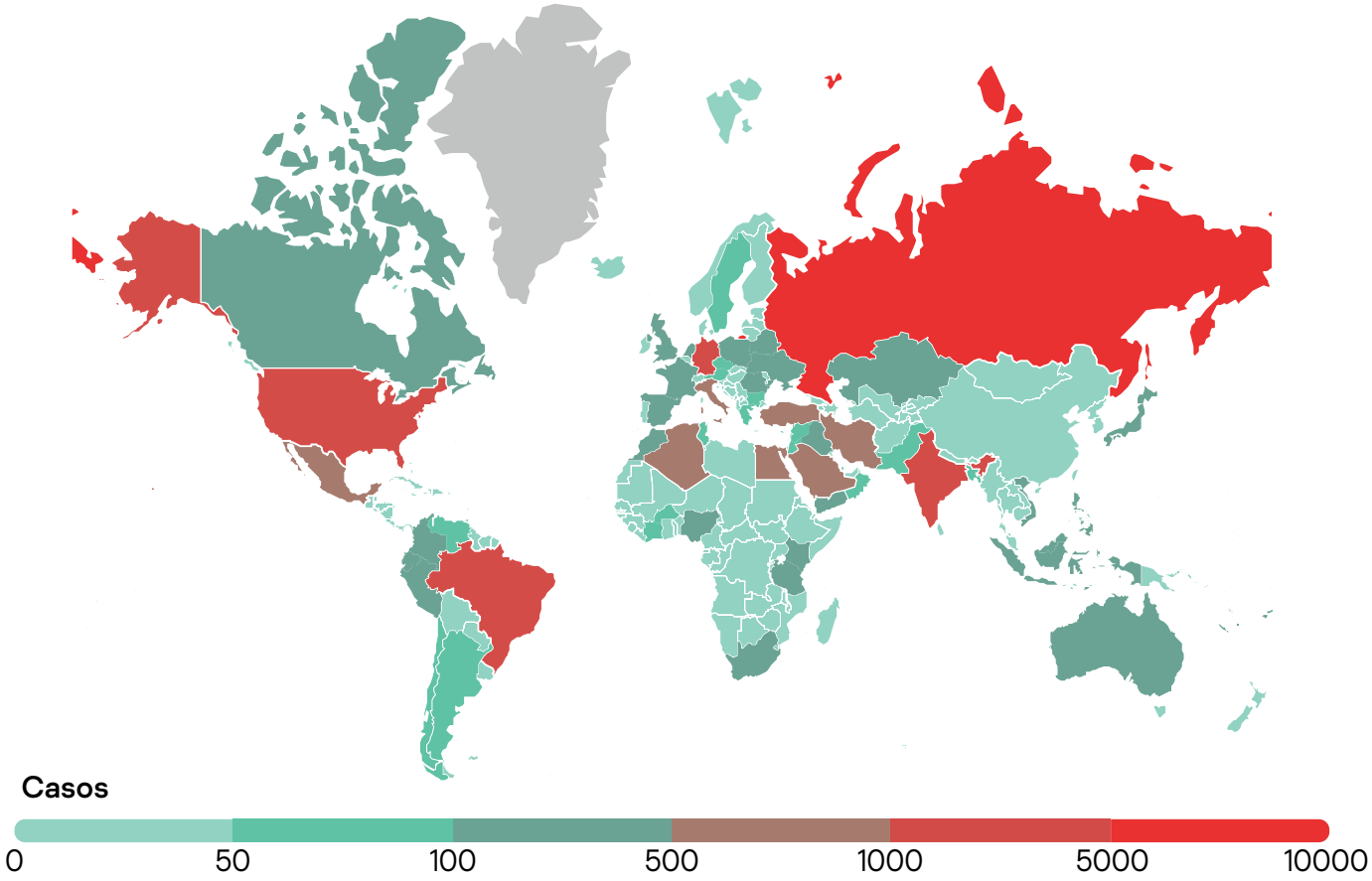
O gráfico abaixo mostra usuários únicos afetados por mês durante o período de 2019-2021. Podemos ver que, em 2021, a tendência foi mais estável do que em 2020, que teve uma queda visível durante os meses mais impactados por lockdowns e medidas de quarentena.



Usuários únicos afetados por mês durante o período de 2019-2021

Números de detecção global e regional: geografia dos usuários afetados

O stalkerware continua afetando pessoas em todo o mundo: em 2021, a Kaspersky detectou usuários afetados em 185 países ou territórios.



Metodologia

Os dados deste relatório foram extraídos de estatísticas de ameaças agregadas obtidas da Kaspersky Security Network. A Kaspersky Security Network é dedicada ao processamento de fluxos de dados relacionados à segurança virtual de milhões de participantes voluntários em todo o mundo. Todos os dados recebidos são anonimizados. Para calcular nossas estatísticas, analisamos a linha de consumidores das soluções de segurança para dispositivos móveis da Kaspersky, aplicando apenas os critérios de detecção da Coalition Against Stalkerware sobre stalkerware. Isso significa que o número de usuários afetados foi alvo apenas de stalkerware. Outros tipos de aplicativos de monitoramento ou spyware que estão fora da definição do Coalition não estão incluídos nas nossas estatísticas.

As estatísticas refletem usuários de dispositivos móveis únicos afetados por stalkerware: isso é diferente do número de detecções. O número de detecções pode ser maior, pois podemos detectar stalkerware várias vezes no mesmo dispositivo do mesmo usuário único se ele decidir não remover o aplicativo após receber nossa notificação.

Por fim, as estatísticas refletem apenas usuários de dispositivos móveis que usam as soluções de segurança de TI da Kaspersky. Alguns usuários podem usar outra solução de segurança virtual em seus dispositivos, enquanto outros não usam nenhuma solução.

Em 2020, Rússia, Brasil, Estados Unidos e Índia são, novamente, os quatro principais países com os usuários afetados mais identificados. Curiosamente, o México caiu do quinto para o nono lugar, e Argélia, Turquia e Egito entraram no top 10. Eles substituíram Itália, Reino Unido e Arábia Saudita, que não estão mais entre os 10 principais países mais afetados por stalkerware.

	País	Usuários afetados
1	Federação Russa	7541
2	Brasil	4807
3	Estados Unidos da América	2319
4	Índia	2105
5	Alemanha	1012
6	Irã (República Islâmica do)	891
7	Argélia	665
8	Turquia	660
9	México	657
10	Egito	640

Tabela 1 – Os 10 principais países de 2021 afetados por stalkerware - globalmente

No relatório deste ano, fornecemos estatísticas regionais mais detalhadas com números para Europa, Ásia-Pacífico, América Latina, América do Norte, Europa Oriental (exceto países da UE), Rússia e Ásia Central, Oriente Médio e África.

Na Europa, o número total de usuários únicos afetados foi de 4.236 em 2021. Alemanha, Itália e Reino Unido estão no topo da lista, repetindo suas primeiras colocações no ano passado. A Áustria foi substituída no top 10 pela Chéquia.

	País	Usuários afetados
1	Alemanha	1012
2	Itália	611
3	Reino Unido da Grã-Bretanha e Irlanda do Norte	430
4	França	410
5	Polônia	321
6	Espanha	321
7	Países Baixos	165
8	Romênia	125
9	Bélgica	94
10	Chéquia	82

Tabela 2 - Os 10 principais países de 2021 afetados por stalkerware - Europa

Na Europa Oriental (exceto países da UE), Rússia e Ásia Central, o número total de usuários únicos afetados foi de 9.207. Os três primeiros países foram Rússia, Ucrânia e Cazaquistão.

	País	Usuários afetados
1	Federação Russa	7541
2	Ucrânia	490
3	Cazaquistão	461
4	Bielorrússia	250
5	Uzbequistão	223
6	Azerbaijão	92
7	República da Moldávia	51
8	Tajiquistão	49
9	Quirguistão	40
10	Turcomenistão	19

Tabela 3 - Os 10 principais países de 2021 afetados por stalkerware - Europa Oriental (exceto países da UE), Rússia e Ásia Central

Na região do Oriente Médio e África, o número total de usuários afetados em toda a região foi de 6.270, com Turquia, Egito e Arábia Saudita tendo os usuários mais afetados.

	País	Usuários afetados
1	Turquia	660
2	Egito	640
3	Arábia Saudita	575
4	Quênia	271
5	África do Sul	240
6	Emirados Árabes Unidos	143
7	Nigéria	123
8	Kuwait	68
9	Omã	58
10	Etiópia	46

Tabela 4 - Os 10 principais países de 2021 afetados por stalkerware - Oriente Médio e África

Na região APAC, o número total de usuários afetados foi de 4.243. A Índia estava substancialmente à frente de outros países com 2.105 usuários únicos afetados. Seguida pela Indonésia e o Vietnã.

	País	Usuários afetados
1	Índia	2105
2	Indonésia	353
3	Vietnã	258
4	Filipinas	240
5	Malásia	229
6	Austrália	205
7	Bangladesh	169
8	Japão	167
9	Paquistão	98
10	Sri Lanka	83

Tabela 5 - Os 10 principais países de 2021 afetados por stalkerware - Ásia-Pacífico

O ranking da região da América Latina e do Caribe foi dominada por um país: Brasil, que representou 72,5% do número total de usuários afetados na região (e responde por cerca de 32% da população da região). O Brasil foi seguido por México e Colômbia. Toda a região teve 6.609 usuários afetados.

	País	Usuários afetados
1	Brasil	4807
2	México	657
3	Colômbia	202
4	Equador	192
5	Peru	179
6	Argentina	90
7	Chile	73
8	Venezuela	58
9	Bolívia	46
10	Haiti	36

Tabela 6 - Os 10 principais países de 2021 afetados por stalkerware - América Latina

Por fim, na América do Norte, os Estados Unidos foram responsáveis por 87% de todos os usuários afetados na região, o que era esperado, já que sua população é dez vezes maior que a do Canadá. O número total de usuários afetados na América do Norte, excluindo o México, que foi incluído nos dados da América Latina, é de 2.666.

	País	Usuários afetados
1	Estados Unidos da América	2319
2	Canadá	347

Tabela 7 - Usuários de 2021 afetados por stalkerware – América do Norte

O sistema operacional Android e o iOS são igualmente afetados pelo stalkerware?

As ferramentas de stalkerware são menos frequentes em iPhones do que em dispositivos Android porque o iOS é tradicionalmente um sistema fechado. No entanto, os agressores podem contornar essa limitação em iPhones com jailbreak, mas ainda exigem acesso físico direto ao telefone para fazer o jailbreak. Os usuários de iPhone que temem vigilância devem sempre ficar de olho no seu dispositivo.

De outra forma, um agressor pode oferecer à vítima um iPhone, ou qualquer outro dispositivo, com stalkerware pré-instalado. Existem muitas empresas que disponibilizam esses serviços online, permitindo que os agressores tenham essas ferramentas instaladas em novos telefones, que podem ser entregues em embalagens de fábrica sob o disfarce de um presente para a vítima planejada.

Funcionalidades comuns de aplicativos stalkerware

Esta seção lista os aplicativos stalkerware mais usados para controlar dispositivos móveis em nível global. Cerberus e Reptilicus foram os aplicativos de stalkerware mais usados, com 5.575 e 4.417 usuários afetados, respectivamente, em todo o mundo.

	Nome do aplicativo	Usuários afetados
1	Cerberus	5,575
2	Reptilicus (também conhecido como 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

Tabela 8 - lista dos principais de aplicativos stalkerware de 2021

Os aplicativos de stalkerware podem fornecer um tremendo poder e acesso a seus usuários, dependendo dos aplicativos e se eles são usados no modo gratuito ou pago. Alguns deles são comercializados como aplicativos antifurto ou de controle parental; no entanto, são diferentes em vários aspectos, começando pelo fato de funcionarem em modo furtivo sem o consentimento e conhecimento da vítima.

A maioria dos aplicativos populares fornece funcionalidades comuns de stalkerware, como:

- Esconder o ícone do aplicativo
- Ler SMS, MMS e registros de chamadas
- Obter as listas de contatos

- Rastrear localização GPS
- Acompanhar eventos do calendário
- Ler mensagens de serviços de mensagens populares e redes sociais, como 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.
- Visualizar fotos e imagens das galerias de imagens dos telefones
- Fazer capturas de tela
- Tirar fotos da câmera frontal (modo selfie)

O uso de stalkerware pode estar diminuindo, mas a violência não

O número de usuários afetados e alguns dos comportamentos e percepções em torno do uso de stalkerware ainda são preocupantes

Embora observemos uma diminuição de 39% nos usuários afetados em nossos dados de 2020, a luta contra o stalkerware e a violência virtual está longe de acabar. O número de usuários afetados e alguns dos comportamentos e percepções em torno do uso de stalkerware ainda são preocupantes. Em novembro de 2021, a Kaspersky realizou uma pesquisa global com mais de 21.000 participantes em 21 países sobre suas atitudes em relação à privacidade e perseguição digital em relacionamentos íntimos. Embora a maioria dos entrevistados (70%) não acredite que seja aceitável monitorar seu parceiro sem consentimento, uma parcela significativa das pessoas (30%) não vê nenhum problema com isso e acha aceitável sob certas circunstâncias. Dos que acham que há razões justificáveis para a vigilância secreta, quase dois terços praticariam esse comportamento se acreditassem que seu parceiro estava sendo infiel (64%) ou se estivesse relacionado à sua segurança (63%) e metade se acreditasse que seu parceiro estava envolvido em atividades criminosas (50%).

As tecnologias de TIC são ferramentas poderosas para os agressores exercerem controle coercitivo, especialmente em relacionamentos em que a violência já está presente offline

A internet de alta velocidade em conjunto com a rápida disseminação da tecnologia da informação e comunicação (TIC) apoiou a violência virtual ao criar outra ferramenta para os agressores compartilharem materiais violentos e perigosos ou se envolverem em comportamentos que afetam danos emocionais, psicológicos ou físicos. Embora essas tecnologias tenham dado às pessoas a capacidade de manter relacionamentos sociais e emocionais em amplas distâncias físicas, a TIC também permitiu a violência virtual, uma consequência cujos efeitos de longo alcance se estendem ao mundo offline com impactos negativos na vida real sobre suas vítimas.

Os resultados da nossa pesquisa corroboram isso, com 15% dos entrevistados em todo o mundo sendo solicitados pelo parceiro a instalar um aplicativo de monitoramento e 34% desses também sofrendo abuso físico e/ou verbal por esse parceiro íntimo.

Embora seja muito cedo para tirar conclusões definitivas sobre a diminuição de usuários afetados em 2021, existem duas teorias que podem explicar essa tendência.

Em primeiro lugar, acreditamos que todos os aspectos das nossas vidas ainda são fortemente impactados pela pandemia. Estudos recentes mostram que novos comportamentos estão surgindo em áreas da vida como trabalho, aprendizado, casa, consumo, comunicação e informação, viagens e mobilidade. Em suma, as pessoas estão ficando mais em casa (49% evitam sair de casa e 50% estão trabalhando em casa parcial ou totalmente), reduzindo as interações face a face (57% indicam que estão se distanciando socialmente dos amigos e da comunidade) e as viagens, além de comprarem, estudarem e se entreterem cada vez mais online. Do ponto de vista de um agressor, isso pode resultar em menos necessidade de espionar seu parceiro, que agora está à vista dele na maior parte do tempo.

Em segundo lugar, a Internet das Coisas (IoT) e a digitalização estão agora em toda parte das nossas vidas. Elas preenchem nossas rotinas diárias e nossas casas, carros e escritórios. Embora as oportunidades e vantagens sejam infinitas, muitos dispositivos também permitem o rastreamento por terceiros. Nossa pesquisa sugere que os agressores também podem usar outros meios, além do stalkerware, para rastrear seus parceiros, com 50% dos entrevistados da nossa pesquisa indicando que foram rastreados através de aplicativos de telefone, outros 29% mencionando que foram rastreados através de dispositivos de rastreamento, 22% através de webcams e 18% através de dispositivos domésticos inteligentes.

A recente publicação da Apple em janeiro de 2022 de um manual de segurança para seu produto AirTag marca uma mudança na percepção da situação.

A NNEDV, a Rede Nacional para Acabar com a Violência Doméstica, e a WWP EN, a Rede Europeia para o Trabalho com Autores de Violência Doméstica, compartilham conosco suas experiências e opiniões sobre essas duas teorias e sobre o abuso de tecnologia em geral.

Como as medidas impostas pelos governos durante a pandemia facilitaram e reforçaram o controle coercitivo dos agressores — Berta Vall Castelló, Gerente de Pesquisa e Desenvolvimento e Anna McKenzie, Gerente de Comunicação da WWP EN

O controle coercitivo é definido como "um padrão de comportamento abusivo projetado para exercer dominação e controle sobre a outra parte de um relacionamento. Ele pode incluir uma série de comportamentos abusivos, como físicos, psicológicos, emocionais ou financeiros, cujo efeito cumulativo ao longo do tempo priva as vítimas sobreviventes da sua autonomia e independência como indivíduo" (McGorrery e McMahon, 2020). Como escrevemos em nosso manual "Same Violence, New Tools – How to work with violent men who use cyberviolence (Mesma Violência, Novas Ferramentas – Como trabalhar com homens violentos que usam a violência virtual)", os agressores isolam suas parceiras e as tornam emocionalmente dependentes. Eles usam agressões, ameaças, intimidação, humilhação, isolamento e muitas outras para criar uma sensação constante de medo, bem como uma perda geral da sensação de liberdade. As tecnologias de TIC são ferramentas poderosas para os agressores exercerem controle coercitivo, especialmente em relacionamentos em que a violência já está presente offline.

Uma análise recente sobre a violência doméstica durante a pandemia de COVID-19 constatou que as medidas impostas pelo governo durante o lockdown facilitam e reforçam o controle coercitivo dos agressores. Os autores sugeriram que as condições de isolamento/distanciamento físico impostas pelos governos se sobrepõem às estratégias de controle coercitivo usadas pelos agressores para controlar seus parceiros (Pentaraki e Speake, 2020). Considerando esses resultados, parece provável que os agressores sintam menos "necessidade" de usar stalkerware para exercer controle coercitivo sobre seus parceiros. Além disso, pesquisas recentes observaram que o abuso facilitado pela tecnologia geralmente aumenta durante um período de separação (George e Harris 2014; Woodlock 2016). Portanto, durante uma situação de lockdown em que os casais foram forçados a ficar juntos em casa, eles são menos propensos a usar o abuso facilitado pela tecnologia.

WWP EN

A Rede Europeia para o Trabalho com Autores de Violência Doméstica (WWP EN) é uma associação de membros de organizações que trabalham direto ou indiretamente com pessoas que cometem violência em relacionamentos íntimos. O foco principal da WWP EN é a violência perpetrada por homens contra mulheres e crianças. A missão da WWP EN é melhorar a segurança das mulheres e dos seus filhos e de outras pessoas que correm risco de violência nas relações íntimas, através da promoção de um trabalho eficaz com aqueles que cometem essa violência, principalmente os homens.

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

Medidas impostas pelo governo durante o lockdown facilitam e reforçam o controle coercitivo dos agressores

Devemos lembrar que uma diminuição no uso de stalkerware não equivale a uma diminuição geral da violência por parceiro íntimo (VPI) durante a pandemia. Pelo contrário, Boxall, Morgan e Brown (2020) observam que a VPI aumentou durante a pandemia de COVID-19. Portanto, os resultados desse relatório indicam que o stalkerware foi substituído por outras ferramentas. Como Elena Gajotto, da ONG italiana Una Casa per l'Uomo, comenta: "É tão fácil monitorar e rastrear alguém, por exemplo, usando sua conta do Google, que você realmente não precisa usar stalkerware". A grande variedade de possíveis abusos facilitados pela tecnologia podem ter impactado especificamente na diminuição do uso de stalkerware. Letizia Baroncelli, da ONG italiana Centro Ascolto Uomo Malttratanti (CAM), concorda e acrescenta: "Acho que vemos menos stalkerware porque existem muitas outras formas de cometer abuso digital".

No entanto, ONGs, governos e pesquisadores relataram um aumento substancial no abuso baseado em imagens e "sextorsão" (extorsão sexual) desde o início da pandemia (Boniello, 2020; CCRI, personal communication, June 2, 2020; FBI, 2020, 2021). Parece que esse tipo de abuso facilitado pela tecnologia aumentou, especialmente entre adolescentes e casais que não moram juntos. Como observa Letizia Baroncelli: "O compartilhamento de fotos pessoais aumentou muito desde que a pandemia começou, especialmente entre jovens agressores. Eles não entendem que estão cometendo um crime". Como Elena Gajotto acrescenta: "O abuso baseado em imagens causa danos devastadores às mulheres que o vivenciam, enquanto os homens nem entendem que fizeram algo ruim".

Vários membros da WWP EN compartilharam que a forma mais comum de violência digital é o monitoramento por homens das atividades digitais de seus parceiras, por exemplo verificando e-mails, telefones e contas de redes sociais. Isso está de acordo com as observações de Daniel Antunovic, da ONG croata UZOR, que concorda que as formas "primitivas" de perseguição digital são as que ele vê com mais frequência.

Na WWP EN, consideramos fundamental focar no abuso facilitado pela tecnologia para garantir a segurança das vítimas. Elena Gajotto acrescenta: "Cerca da metade dos homens compartilham sua violência digital, sem perceber que isso é abuso. Se não focarmos explicitamente nessa violência em nosso trabalho com os agressores, ela não surgirá". Portanto, há necessidade de aumentar a capacidade dos profissionais que trabalham com agressores e profissionais que trabalham com

vítimas de violência doméstica para rastrear e intervir em casos de violência digital. Como Daniel Antunovic acrescenta: "Não encontramos tantos casos de violência digital quanto eu esperava desde o COVID-19. No entanto, o abuso facilitado pela tecnologia é, de certa forma, como violência sexualizada. Acontece muito, mas fica escondido".

NNEDV

O Projeto Rede de Segurança da NNEDV se concentra na interseção entre tecnologia, privacidade, confidencialidade e inovação, no que se refere à segurança e ao abuso, defendendo políticas, educando e treinando defensores e profissionais do sistema de justiça e trabalhando com comunidades, agências e empresas de tecnologia para responder ao abuso tecnológico, apoiar os sobreviventes em seu uso da tecnologia e aproveitar a tecnologia para melhorar os serviços.

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

Há uma taxa crescente de "dispositivos inteligentes" usados na violência entre parceiros íntimos — Toby Shulruff, Gerente de Projetos de Segurança Técnica da NNEDV

Embora o stalkerware seja uma preocupação comum, existem muitas outras ferramentas disponíveis para abuso tecnológico que podem parecer stalkerware, mas não são. Por exemplo, as informações pessoais disponíveis online e os recursos diários de dispositivos e contas podem ser usados para encontrar a localização de uma pessoa ou rastrear sua atividade. A complexidade e as conexões entre dispositivos, contas e informações na Internet podem dificultar a avaliação do que está acontecendo e a implementação de uma resposta eficaz para as vítimas e para quem trabalha com elas. Pode ser aterrorizante e avassalador para um sobrevivente perceber que um agressor conhece vários detalhes sobre sua vida cotidiana.

Infelizmente, há uma taxa crescente de dispositivos "inteligentes", incluindo assistentes domésticos, aparelhos conectados e sistemas de segurança conectados a redes Wi-Fi e smartphones, usados na violência entre parceiros íntimos.

Em uma pesquisa realizada pela NNEDV em dezembro de 2020 e janeiro de 2021, as respostas revelaram um aumento em todos os tipos de abuso de tecnologia durante a pandemia. Embora os telefones sejam a tecnologia mal utilizada com mais frequência, a avaliação de necessidades da NNEDV mostra que este é o caso em 87% das vezes, dispositivos "inteligentes" ou conectados também foram identificados como tecnologias que são cada vez mais mal utilizadas no contexto do abuso de tecnologia, observado regularmente por cerca de um terço dos profissionais de suporte.

Há uma taxa crescente de dispositivos "inteligentes", incluindo assistentes domésticos, aparelhos conectados e sistemas de segurança conectados a redes Wi-Fi e smartphones, usados na violência entre parceiros íntimos

À medida que mais pessoas adotam o uso de dispositivos IoT, isso provavelmente aumentará. Estes produtos destinam-se a aumentar a praticidade e a eficiência. A fabricação de dispositivos IoT é um mercado global que aumenta rapidamente, com players maiores e bem estabelecidos, bem como muitas empresas menores e mais novas[1]. A IoT é possibilitada por várias tendências sobrepostas na tecnologia: miniaturização, aumento da capacidade de processamento, aumento do armazenamento de dados, diminuição do custo de fabricação e conectividade.

Devido a uma variedade de fatores, como pressões do mercado, o rápido desenvolvimento da tecnologia e a complexidade da IoT, riscos profundos à segurança e à privacidade são cada vez mais aparentes[2]. Dispositivos domésticos inteligentes, em particular, estão sendo mal utilizados no contexto de violência por parceiro íntimo para controlar, ameaçar e causar danos às vítimas. [Pesquisadores do projeto Gender + IoT da University College London[3] vêm explorando esses danos] [e propondo soluções em parceria com profissionais de suporte na área.]

A recente avaliação de necessidades da NNEDV documentou aumentos nas táticas de abuso de tecnologia durante a pandemia. Estamos preocupados que, ao sairmos dessa crise de saúde pública, os abusadores que adotaram essas táticas ou aumentaram o uso indevido da tecnologia durante esse período não terão nenhum incentivo para interromper essa forma de abuso. Pesquisas[4] recentes sugerem que os profissionais de suporte devem perguntar sobre todos os tipos de abuso de tecnologia, incluindo stalkerware e dispositivos domésticos inteligentes. Há uma alta probabilidade de que o aumento no número de profissionais de suporte relacionado a abuso tecnológico permaneça conosco. É imperativo que continuemos a apoiar as vítimas e trabalhemos para evitar o abuso tecnológico.

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 ou 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 ou https://www.internetsociety.org/iot/

3 Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). The rise of the Internet of Things and implications for technology-facilitated abuse. University College London.

4 Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. Proceedings of the ACM on human-computer interaction, 1 (CSCW), p.1-22.

Como a Kaspersky e seus parceiros estão colaborando para combater o stalkerware

A ameaça do stalkerware não é apenas um problema técnico: todas os setores da sociedade precisam estar envolvidas na resolução do problema. Nos últimos anos, a Kaspersky tem estado na vanguarda do debate sobre stalkerware. Estamos entrando em contato com as partes interessadas públicas e privadas para entender melhor esse problema e encontrar soluções comuns. Estamos contribuindo para o desenvolvimento de materiais de treinamento e ferramentas práticas para apoiar organizações sem fins lucrativos, corporações, instituições e indivíduos no desenvolvimento de resiliência ao stalkerware. Estamos organizando e participando de webinars e mesas redondas com instituições para compartilhar nossas vozes e contribuir para as discussões que moldarão a legislação do futuro.

A Kaspersky é uma dos cofundadoras e impulsionadoras da Coalition Against Stalkerware (CAS), um grupo de trabalho internacional dedicado a combater o stalkerware e a violência doméstica. A coalizão reúne organizações que trabalham com vítimas e agressores, ativistas digitais e fornecedores de segurança virtual. É uma plataforma única que permite a todas as partes interessadas compartilharem as melhores práticas e unirem forças para enfrentar a questão do stalkerware.

A Kaspersky também é uma das parceiras do projeto DeStalk. Financiado pela Comissão Europeia, esse projeto de pesquisa visa desenvolver uma estratégia para treinar e apoiar profissionais que trabalham em serviços de apoio às vítimas e programas para agressores, funcionários de instituições e governos locais, juntamente com outros grupos relevantes. O consórcio planeja atualizar e testar as ferramentas existentes para os profissionais e está desenvolvendo uma campanha de conscientização regional piloto na Itália.

Em 2021, nos unimos à INTERPOL e a duas respeitadas organizações sem fins lucrativos dos EUA e da Austrália para fornecer às autoridades policiais duas sessões de treinamento online. Mais de 210 participantes de todo o mundo compareceram ao curso.

No final de 2021, a Kaspersky também participou de um evento chamado "Combate à violência contra as mulheres na era digital — utilizando a Convenção de Istambul", organizado pelo Conselho da Europa. Esse evento foi uma oportunidade para discutir as recomendações do Grupo de Peritos no Combate à Violência contra a Mulher e à Violência Doméstica (GREVIO).

TinyCheck: uma ferramenta de apoio às vítimas de violência doméstica

O trabalho da Kaspersky com a ferramenta TinyCheck é uma iniciativa que merece destaque. É uma ferramenta gratuita e de código aberto desenvolvida e suportada pela Kaspersky. Inicialmente criado para ajudar as organizações sem fins lucrativos a proteger as vítimas de violência doméstica e sua privacidade, o TinyCheck facilita a detecção de stalkerware nos dispositivos das vítimas e em qualquer sistema operacional de maneira simples, rápida e não invasiva, sem alertar o agressor. Embora as soluções de segurança também possam verificar e alertar sobre stalkerware, elas precisam ser instaladas no dispositivo, então existe o risco de o agressor também ser alertado. Desenvolvimentos como a ferramenta TinyCheck visam garantir que os sobreviventes possam usar seus dispositivos sem a preocupação de serem vigiados.

TinyCheck facilita a detecção de stalkerware nos dispositivos das vítimas e em qualquer sistema operacional de maneira simples, rápida e não invasiva, sem alertar o agressor

Com o TinyCheck, nenhum aplicativo precisa ser instalado no dispositivo para realizar a verificação, e os resultados da verificação não são exibidos ou transmitidos para o dispositivo possivelmente infectado. Além disso, o TinyCheck permite que as vítimas verifiquem qualquer dispositivo, independentemente de usar iOS, Android ou outro sistema operacional. Esses recursos abordam os dois principais problemas na luta para proteger os usuários contra o stalkerware. A ferramenta foi desenvolvida para rodar em um Raspberry Pi, usando uma conexão Wi-Fi regular. O TinyCheck analisa rapidamente o tráfego de saída de um dispositivo móvel e identifica indicadores de comprometimento (IOCs), como interações com fontes maliciosas conhecidas, como servidores relacionados a stalkerware. Atualmente, a ferramenta usa IOCs coletados não apenas por pesquisadores da Kaspersky, mas também por repositórios mantidos por pesquisadores de segurança independentes (agradecimentos especiais a Etienne Maynier, também conhecido como Tek, da Echap e Cian Heasley). Esperamos que a comunidade continue esse trabalho mantendo os IOCs atualizados.

Dito isso, as limitações do TinyCheck precisam ser compreendidas. A ferramenta deve ser usada com o seguinte aviso em mente: os IOCs não fornecem detecção completa em tempo real de todos os aplicativos de stalkerware, como uma solução de segurança de TI faz. Portanto, um resultado que não detecte nenhum stalkerware não exclui a possibilidade de que o stalkerware tenha sido instalado, mas não detectado pelo TinyCheck.

Em 2021, mais organizações sem fins lucrativos no campo da violência doméstica testaram o TinyCheck e forneceram feedback para ajudar a melhorar o serviço. As forças policiais e os órgãos judiciais de vários países também se interessaram pela ferramenta para melhor apoiar as vítimas.

2021 teve desenvolvimentos positivos nas frentes de regulamentação e institucional

Em todo o mundo, 2021 observou alguns desenvolvimentos positivos na luta contra o stalkerware do ponto de vista regulatório e institucional. Em maio de 2021, o Diet, o parlamento do Japão, promulgou um projeto de lei para alterar sua regulamentação contra perseguidores. De acordo com a lei revisada, além de outras estipulações, obter informações de localização de smartphones de pessoas por meio de aplicativos sem autorização agora é ilegal.

Em agosto de 2021, a Comissão Federal de Comércio dos Estados Unidos proibiu um fabricante de aplicativos de oferecer stalkerware. Foi a primeira proibição desse tipo.

Em 17 de agosto de 2021, o Bundestag alemão aprovou a "Lei de Alteração do Código Penal — Combate Mais Eficaz à Perseguição e Melhor Cobertura contra a Perseguição Virtual" (traduzido do alemão). A nova lei entrou em vigor em 1º de outubro de 2021 e agora inclui perseguição virtual em seu catálogo de crimes. A mudança se deve ao progresso tecnológico contínuo e ao aumento associado de perseguição virtual, particularmente através de aplicativos de perseguição ou stalkerware. Além disso, uma parte importante da nova lei é que ela classifica um caso como grave se o infrator "no curso de uma infração, usar um programa de computador cuja finalidade é a espionagem digital de outras pessoas".

O Conselho da Europa tem sido muito ativo neste tópico em 2021. Na sua primeira recomendação sobre a "dimensão digital" da violência contra as mulheres, o Grupo de Peritos do Conselho da Europa em Ação contra a Violência contra as Mulheres e a Violência Doméstica (GREVIO) define e descreve os problemas da violência de gênero contra as mulheres cometida online e ataques habilitados por tecnologia contra mulheres, como dispositivos de rastreamento legalmente obtidos que permitem que os agressores persigam suas vítimas. Logo depois, em dezembro de 2021, foi publicado um relatório de iniciativa legislativa sobre violência de gênero virtual que foi adotado pelo Parlamento Europeu. O relatório pede (i) uma definição comum de violência de gênero virtual e (ii) capacitação para as partes interessadas. Ele destaca o stalkerware entre os principais métodos de violência cibernética e "descarta a noção de que os aplicativos stalkerware podem ser considerados aplicativos de controle parental". Seguindo as recomendações gerais do Conselho da Europa, esse

relatório, embora não vinculativo, é mais um documento oficial positivo que destaca a questão do stalkerware e pressiona os Estados europeus a adaptarem suas legislações e ações para combater o problema. Enfim, em 8 de março de 2022, a Comissão Europeia publicou uma proposta de Diretiva do Parlamento Europeu e do Conselho sobre o combate à violência contra as mulheres e à violência doméstica. O documento aborda a violência virtual e dedica dois artigos à perseguição virtual (Art. 8°) e ao assédio virtual (Art. 9°) que propõe criminalizar.

Acredita ser vítima de stalkerware? Aqui estão algumas dicas

Se você precisar de ajuda, procure uma organização de apoio. Para encontrar uma perto de você, consulte o site da Coalizão Contra o Stalkerware

Se você é ou não vítima de stalkerware, aqui estão algumas dicas caso queira se proteger melhor:

- Proteja seu telefone com uma senha forte que você nunca compartilha com seu parceiro, amigos ou colegas
- Altere as senhas de todas as suas contas periodicamente e não as compartilhe com ninguém
- Baixe apenas aplicativos de fontes oficiais, como Google Play ou Apple App Store
- Instale uma solução de segurança de TI confiável como o Kaspersky Internet Security para Android nos dispositivos e verifique-a regularmente. No entanto, no caso de stalkerware possivelmente já instalado, isso só deve ser feito após a avaliação do risco para a vítima, pois o agressor pode perceber o uso de uma solução de segurança cibernética.

As vítimas de stalkerware podem ser vítimas de um ciclo maior de abuso, inclusive físico. Em alguns casos, o agressor é notificado se a vítima realizar uma varredura no dispositivo ou remover um aplicativo stalkerware. Se isso acontecer, pode levar a uma escalada da situação e mais agressão. Por isso que é importante proceder com cautela se você acha que está sendo alvo de stalkerware.

- **Entre em contato com uma organização de suporte local:** para encontrar uma perto de você, consulte o site da Coalition Against Stalkerware.
- **Preste atenção aos seguintes sinais de alerta:** entre eles, podem-se incluir uma bateria que descarrega rapidamente devido a aplicativos desconhecidos ou suspeitos que consomem sua carga e aplicativos recém-instalados com acesso suspeito para usar e rastrear sua localização, enviar ou receber mensagens de texto e outras atividades pessoais. Verifique também se a configuração de "fontes desconhecidas" está habilitada, pode ser um sinal de que um software indesejado foi instalado de uma fonte de terceiros. É importante notar que os sinais acima são apenas sintomas de uma possível instalação de stalkerware, não uma indicação definitiva.
- **Não tente apagar o stalkerware, alterar qualquer configuração ou adulterar seu telefone:** isso pode alertar seu possível agressor e levar a uma escalada da situação. Você também corre o risco de apagar dados ou provas importantes que podem ser usados em um processo judicial.

Para mais informações sobre nossas atividades contra o stalkerware ou para fazer uma solicitação, envie uma mensagem para ExtR@kaspersky.com.

A Coalizão Contra o Stalkerware foi fundada em novembro de 2019 em resposta à ameaça crescente do stalkerware. A Coalizão busca combinar a experiência de seus parceiros em apoio a sobreviventes de violência doméstica e de agressores, defesa dos direitos digitais e defesa dos direitos digitais de crimes causados pelo stalkerware. Todos os membros têm o compromisso de combater a violência doméstica, perseguição e assédio ao enfrentar o stalkerware e informar o público sobre o problema.

A Coalizão Contra o Stalkerware:
https://stopstalkerware.org/

COALITION AGAINST STALKERWARE

Notícias sobre ciberameaças: www.securelist.com
Notícias sobre segurança da informação: business.kaspersky.com
Segurança para empresas pequenas e médias: www.kaspersky.com.br/small-to-medium-business-security
Segurança para empresas grandes: www.kaspersky.com.br/enterprise-security

www.kaspersky.com.br

kaspersky