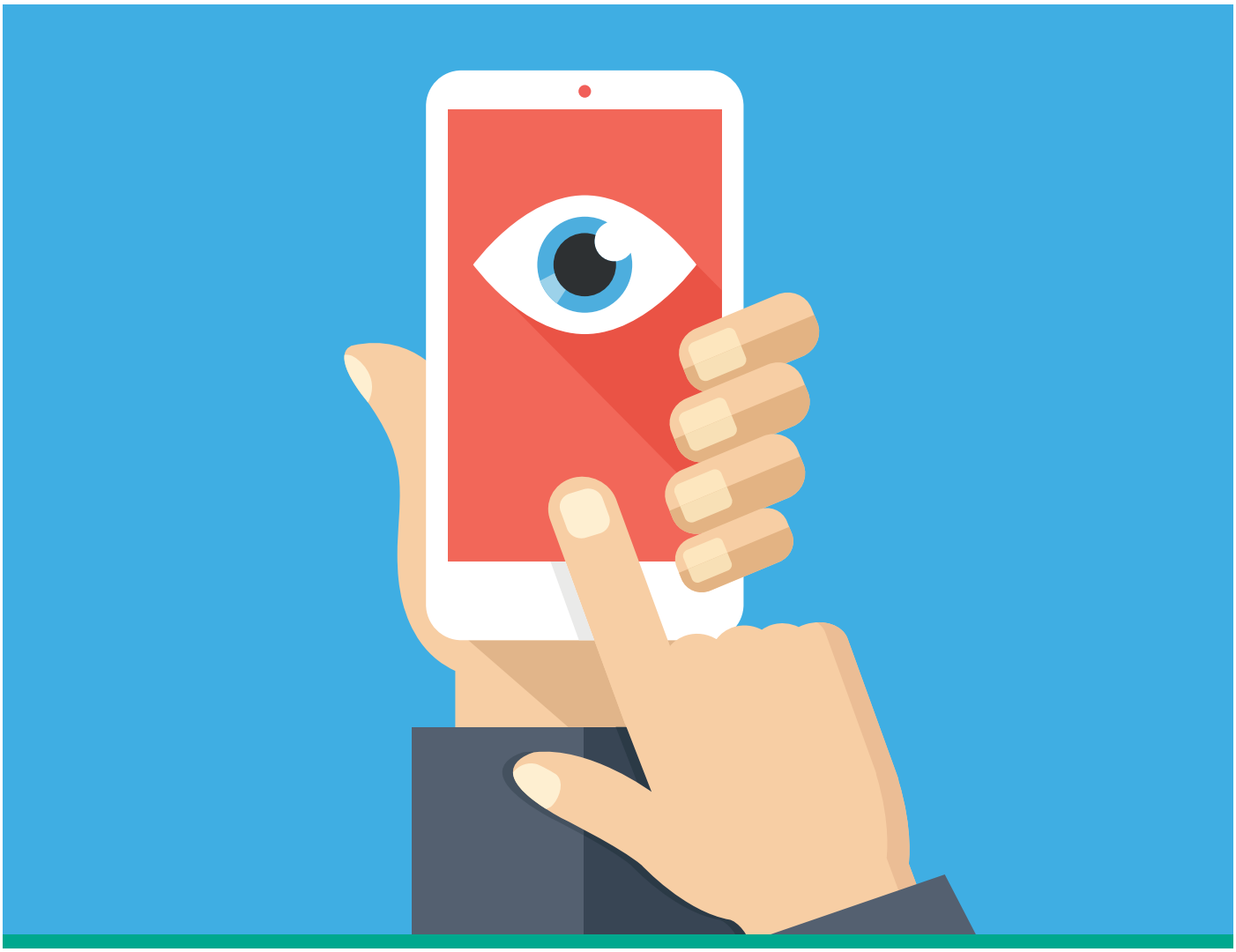


O Estado do **Stalkerware** em 2020

COALITION AGAINST STALKERWARE

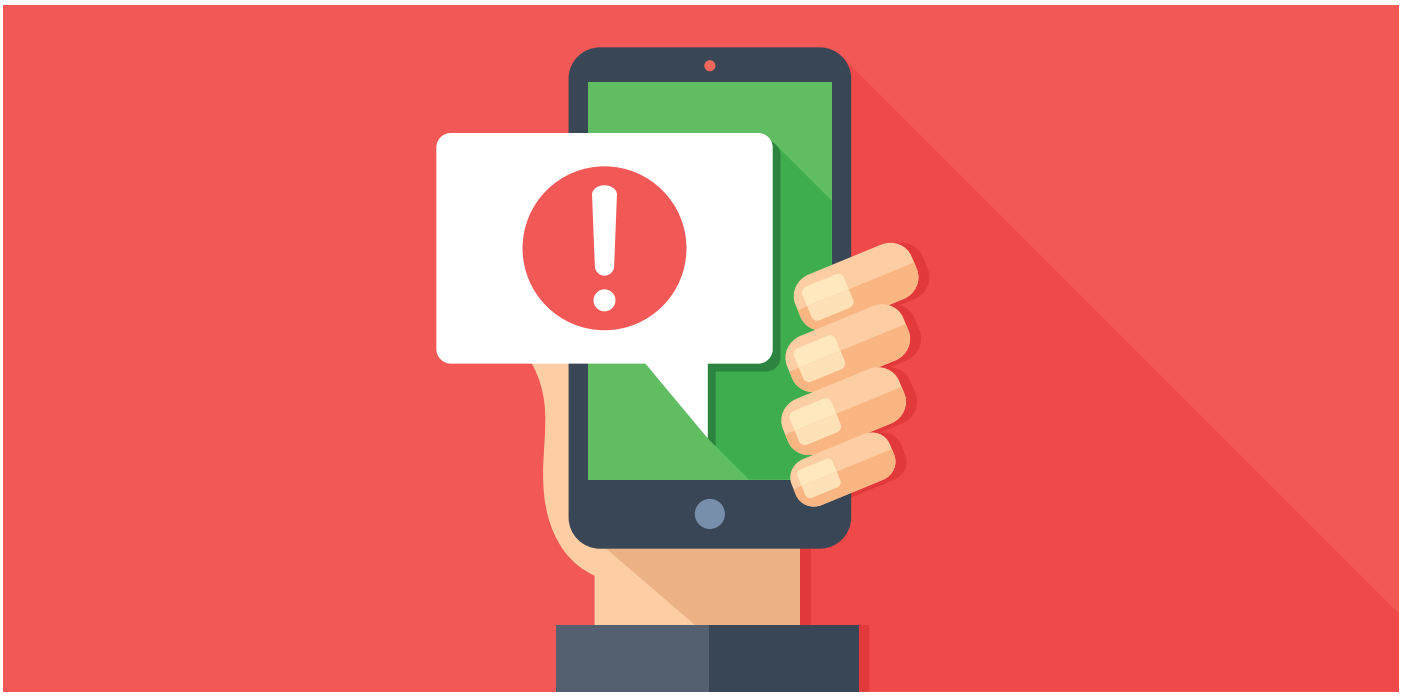
kaspersky

Índice

Principais descobertas em 2020

Os dados da Kaspersky mostram que a dimensão do problema de stalkerware não melhorou muito em 2020 em comparação com o ano anterior:

- o número de pessoas afetadas ainda é alto. No total, 53.870 de nossos usuários móveis foram afetados globalmente por stalkerware em 2020. Pensando no quadro geral, esses números incluem apenas os usuários da Kaspersky, o que significa que os números globais totais são maiores. Alguns usuários afetados podem usar outra solução de segurança cibernética em seus dispositivos, enquanto alguns não usam nenhuma solução.
- Com mais de 8.100 usuários afetados globalmente, o Nidb é a amostra de stalkerware mais usada, de acordo com nossas estatísticas de 2020. Essa amostra é usada para vender vários produtos de stalkerware diferentes, como iSpyoo, TheTruthSpy e Copy9, entre outros.
- Em termos de distribuição geográfica, vemos o surgimento de uma tendência bastante consistente: a Rússia, o Brasil e os Estados Unidos da América (EUA) continuam a ser os países mais afetados globalmente e são os três países líderes em 2020.
- Na Europa, Alemanha, Itália e Reino Unido são os três países mais afetados, respectivamente.



Introdução e metodologia

A tecnologia permitiu que as pessoas se conectassem mais do que nunca. Podemos escolher compartilhar digitalmente nossas vidas com nosso parceiro, familiares e amigos, independentemente da nossa distância física. No entanto, também vemos um crescimento em software que permite aos usuários espionar remotamente a vida de outra pessoa por meio de seu dispositivo digital, sem que o usuário afetado dê seu consentimento ou seja notificado.

Os riscos do stalkerware podem ir além da esfera online e entrar no mundo físico. A Coalition Against Stalkerware adverte que o stalkerware "pode facilitar a vigilância, assédio, abuso, perseguição e/ou violência contra o parceiro".

Esse software, conhecido como stalkerware, está disponível comercialmente para todos com acesso à internet. Os riscos do stalkerware podem ir além da esfera online e entrar no mundo físico. A Coalition Against Stalkerware adverte que o stalkerware "pode facilitar a vigilância, assédio, abuso, perseguição e/ou violência contra o parceiro". O stalkerware também pode operar em modo invisível, o que significa que não há nenhum ícone exibido no dispositivo para indicar sua presença e que ele não é visível para o usuário afetado. A maioria dos usuários afetados nem sabe que esse tipo de software existe. Isso significa que eles não podem se proteger, online ou offline, especialmente porque o infrator que usa stalkerware geralmente conhece sua vítima pessoalmente.

Nos últimos anos, a Kaspersky tem trabalhado ativamente com parceiros para acabar com o uso de stalkerware. Em 2019, criamos um alerta especial que notifica os usuários se o stalkerware estiver instalado em seus telefones. Depois disso, nos tornamos um dos dez membros fundadores da Coalition Against Stalkerware. Também publicamos nosso primeiro relatório completo sobre o estado do stalkerware no mesmo ano para entender a dimensão do problema.

Este relatório continua a examinar a questão do stalkerware e apresenta novas estatísticas de 2020, em comparação com nossos dados anteriores. Os dados neste relatório foram obtidos a partir de estatísticas de ameaças agregadas da Kaspersky Security Network. A Kaspersky Security Network se dedica a processar fluxos de dados relacionados à segurança cibernética de milhões de participantes voluntários em todo o mundo. Todos os dados recebidos são anonimizados. Para calcular nossas estatísticas, revisamos a linha do consumidor de soluções de segurança móvel da Kaspersky.

O problema e a história por trás do stalkerware

O stalkerware é um tipo de software que está disponível comercialmente para todos com acesso à internet. Ele é usado para espionar remotamente a vida de outra pessoa por meio de seu dispositivo, sem que o usuário afetado dê seu consentimento ou seja notificado. O salkerware opera em modo invisível, o que significa que não há nenhum ícone exibido no dispositivo para indicar sua presença e que ele não é visível para o usuário afetado. Por isso, a Coalition Against Stalkerware define o stalkerware como um tipo de software que "pode facilitar a vigilância, assédio, abuso, perseguição e/ou violência contra o parceiro".

A dimensão da violência cibernética

Sete em cada dez mulheres na Europa que sofreram perseguição cibernética também sofreram pelo menos uma forma de violência física e/ou sexual de um parceiro.

De acordo com um relatório do Instituto Europeu para a Igualdade de Gênero, "sete em cada dez mulheres na Europa que sofreram perseguição cibernética também sofreram pelo menos uma forma de violência física e/ou sexual de um parceiro". Reiterando essas descobertas, os especialistas de organizações sem fins lucrativos (ONGs) que ajudam sobreviventes e vítimas de violência doméstica enfatizam que o cyberstalking também é uma forma de violência. Assim como acontece com a violência física, psicológica e econômica, um agressor pode usar a vigilância para obter o controle total de sua vítima/sobrevivente[1] e ficar no controle da situação.

Usando stalkerware, a extensão do controle do agressor pode ser imensa. Dependendo do tipo instalado, o stalkerware pode ter uma variedade de funções para invadir a privacidade da vítima. Com ajuda do software, um agressor pode:

- Ler tudo que a pessoa violada digita – registrando cada tecla no dispositivo, incluindo credenciais para qualquer tipo de serviço, como aplicativos bancários, lojas online e redes sociais, etc.
- Saber onde ela está – rastreando os movimentos de uma pessoa com GPS, em tempo real
- Ouvir o que ela dizem – escutando chamadas ou mesmo gravando-as
- Ler mensagens em qualquer programa de troca de mensagens, independentemente da criptografia usada
- Monitorar atividades em redes sociais

1 Os especialistas referem-se cada vez mais ao termo "sobrevivente" em vez de "vítima" em sua terminologia. Portanto, neste relatório, usaremos os dois termos.

- Ver fotos e vídeos
- Ligar a câmera

Todas essas informações privadas podem ser coletadas, geralmente de um dispositivo móvel, como um tablet ou smartphone.

Organizações sem fins lucrativos da Coalition Against Stalkerware estão vendo um número crescente de sobreviventes procurando ajuda para o problema.

Organizações sem fins lucrativos da Coalition Against Stalkerware estão vendo um número crescente de sobreviventes procurando ajuda para o problema:

- Descobertas da Segunda Pesquisa Nacional sobre abuso de tecnologia e violência doméstica na **Austrália**, lançada pela Rede de Serviços para Mulheres (WESNET) com a assistência da dra. Delanie Woodlock e pesquisadores da Curtin University, afirmam que 99,3% dos praticantes de violência doméstica têm clientes que sofrem abuso facilitado pela tecnologia e que o uso de câmeras de vídeo aumentou 183,2% entre 2015 e 2020.
- De acordo com um estudo sobre violência cibernética nas relações íntimas conduzido pelo Centre Hubertine Auclert na **França**, 21% das vítimas tiveram uma experiência com stalkerware nas mãos de seu parceiro abusivo, e 69% das vítimas têm a sensação de que as informações pessoais em seu smartphone foram acessadas por seu parceiro de forma oculta.
- Na **Alemanha**, por vários anos, Centros de Aconselhamento a Mulheres e Centros de Crise de Estupro (bff) notaram um uso crescente de stalkerware em combinação com relacionamentos amorosos.
- Nos **EUA**, o stalking afeta cerca de 6-7,5 milhões de pessoas por ano, e uma em cada quatro vítimas relata ter sido perseguida por meio de algum tipo de tecnologia, de acordo com o Stalking Prevention Awareness & Resource Center (SPARC).

O acesso físico é a chave

Infelizmente, não é muito difícil instalar secretamente um stalkerware no telefone da vítima. A principal barreira que existe é que o stalkerware precisa ser configurado em um dispositivo afetado. Devido ao vetor de distribuição de tais aplicativos, que são muito diferentes dos esquemas comuns de distribuição de malware, é impossível ser infectado por um stalkerware por meio de uma mensagem de spam, incluindo um link para stalkerware ou uma armadilha por meio da navegação na web.

Isso significa que o abusador precisará ter acesso físico ao dispositivo para instalar o stalkerware. Isso é possível se o dispositivo não tiver um código, padrão ou senha para protegê-lo ou, alternativamente, se o agressor conhecer pessoalmente a vítima/o sobrevivente. A instalação no dispositivo pode ser concluída em poucos minutos.

Antes de acessar o dispositivo do sobrevivente, o agressor precisa coletar um link para o pacote de instalação na página do desenvolvedor de stalkerware. Na maioria dos casos, o software não é baixado de uma loja oficial de aplicativos. Para dispositivos Android, o Google baniu aplicativos que são claramente stalkerware de sua loja de aplicativos Google Play em 2020. Isso significa que o agressor não poderá instalar tal aplicativo da loja de aplicativos geral. Em vez disso, o agressor precisa seguir várias etapas antes de poder instalar o stalkerware. Como resultado, o agressor pode deixar rastros nas configurações do dispositivo que o usuário pode verificar se estiver preocupado com a possibilidade de espionagem.

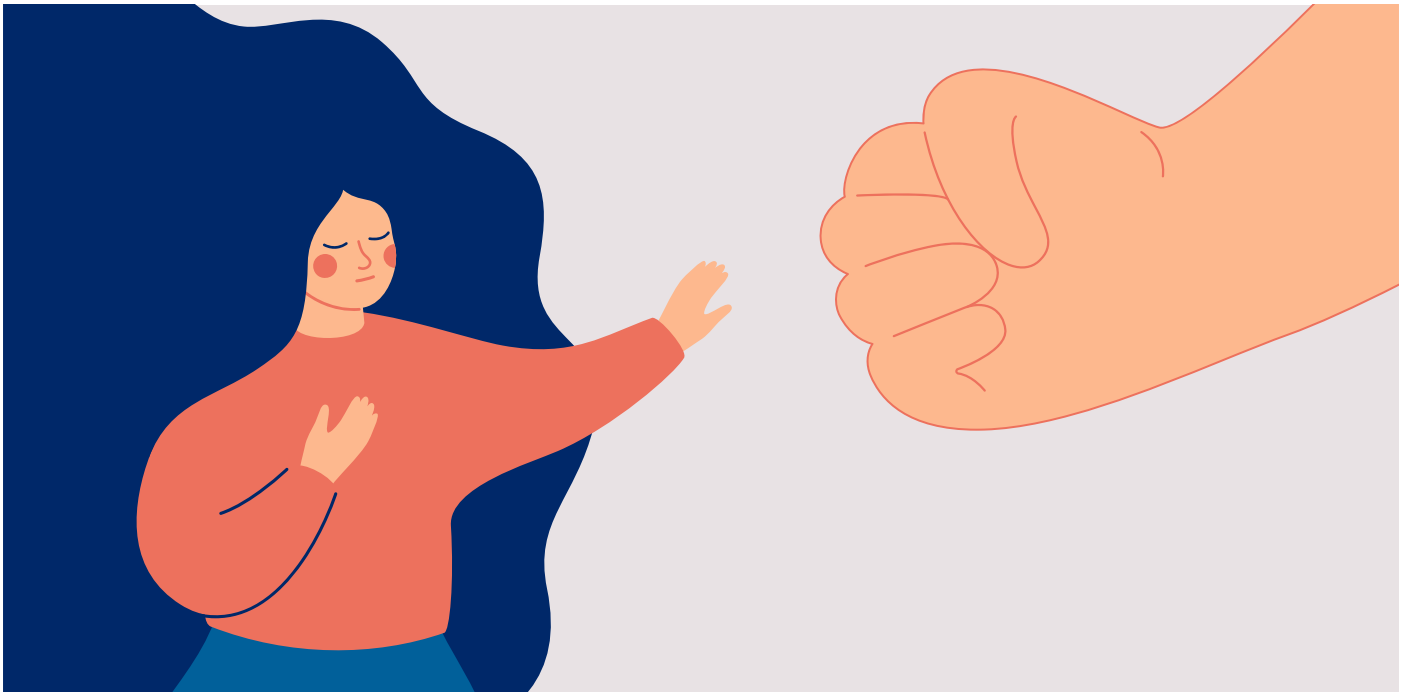
Ferramentas de stalkerware são menos frequentes em iPhones do que em dispositivos Android.

Ferramentas de stalkerware são menos frequentes em iPhones do que em dispositivos Android porque o iOS é tradicionalmente um sistema fechado. No entanto, os infratores podem contornar essa limitação em iPhones com jailbreak. Eles ainda precisam de acesso físico ao telefone para fazer o jailbreak, então os usuários do iPhone que temem vigilância devem sempre ficar de olho em seus dispositivos. Como alternativa, o agressor pode oferecer à vítima um iPhone – ou qualquer outro dispositivo – com stalkerware pré-instalado como presente. Existem muitas empresas que disponibilizam seus serviços online para instalar essas ferramentas em um novo telefone e entregá-lo a um destinatário desinformado em uma embalagem de fábrica para comemorar uma ocasião especial.

O risco de vazamentos de privacidade

As informações monitoradas por meio de stalkerware estarão disponíveis para pelo menos uma pessoa – o agressor que instalou o stalkerware no telefone do sobrevivente. No entanto, às vezes é possível que todos os dados privados se tornem publicamente disponíveis. Ano após ano, servidores de stalkerware são hackeados ou deixados abertos e desprotegidos, de forma que as informações podem ser acessadas e vazadas online. Por exemplo, em 2020, tal violação de dados ocorreu devido a um produto fornecido pela ClevGuard. Nos anos anteriores, vimos incidentes semelhantes com o Mobiispy em 2019 e com o MSpy em 2018 e 2015.

Esses são apenas alguns exemplos de uma longa lista em que bancos de dados de empresas que desenvolvem stalkerware foram expostos, afetando milhões de contas de usuários. Com a possibilidade de rastrear a localização de uma pessoa, isso significa que, além de perder sua privacidade cibernética, as pessoas afetadas podem correr riscos de segurança no mundo físico.



A situação jurídica

Aplicativos de stalkerware são vendidos e fornecidos por empresas com várias fachadas, como soluções de monitoramento de crianças ou rastreamento de funcionários. Embora as leis variem de um país e estado para outro, elas estão se atualizando. De modo geral, só é ilegal usar ferramentas e aplicativos que registrem a atividade do usuário sem o consentimento do usuário ou de uma autoridade jurídica. Lentamente, estamos vendo algumas mudanças na legislação. Por exemplo, em 2020, a França reforçou as sanções ao monitoramento secreto: a geolocalização de alguém sem o seu consentimento agora é passível de punição com um ano de prisão e uma multa de 45.000 euros. Se isso for feito no âmbito de um casal, as sanções são potencialmente mais altas, incluindo dois anos de prisão e uma multa de 60.000 euros.

As ferramentas de stalkerware muitas vezes violam leis e responsabilizam o stalker legalmente por qualquer gravação feita sem o conhecimento da vítima. Stalkers devem perceber que estão infringindo a lei. Se o uso de stalkerware for relatado, a punição se aplica ao infrator que instalou o software – não ao seu fornecedor. Nos EUA, apenas dois desenvolvedores de aplicativos de stalking foram multados no passado recente. Um deles teve que pagar uma multa recorde de 500.000 dólares, o que encerrou o processo de desenvolvimento do aplicativo, enquanto o outro terminou apenas com uma ordem de alterar a funcionalidade do aplicativo para vendas futuras.

A dimensão do problema

Números de detecção globais – usuários afetados

No total, 53.870 usuários individuais foram afetados globalmente por stalkerware em 2020. Já em 2019, 67.500 usuários individuais foram afetados globalmente.

Nesta seção, veremos os números globais de usuários cujos dispositivos móveis foram detectados com stalkerware.

Os dados de 2020 mostram que a situação do stalkerware não melhorou muito: o número de pessoas afetadas ainda é alto. No total, 53.870 usuários individuais foram afetados globalmente por stalkerware em 2020. Já em 2019, 67.500 usuários individuais foram afetados globalmente. No entanto, é preciso levar em conta o fato de que 2020 foi um ano sem precedentes em que as vidas mudaram completamente em todo o mundo.

Para combater a pandemia da COVID-19, todos os países do mundo enfrentaram restrições massivas, como medidas de autoisolamento ou lockdowns para fazer as pessoas ficarem em casa. Considerando que o stalkerware é usado como outra

ferramenta para controlar um parceiro com quem o agressor vive no dia a dia, isso pode explicar os números um pouco mais baixos em comparação com o ano anterior.

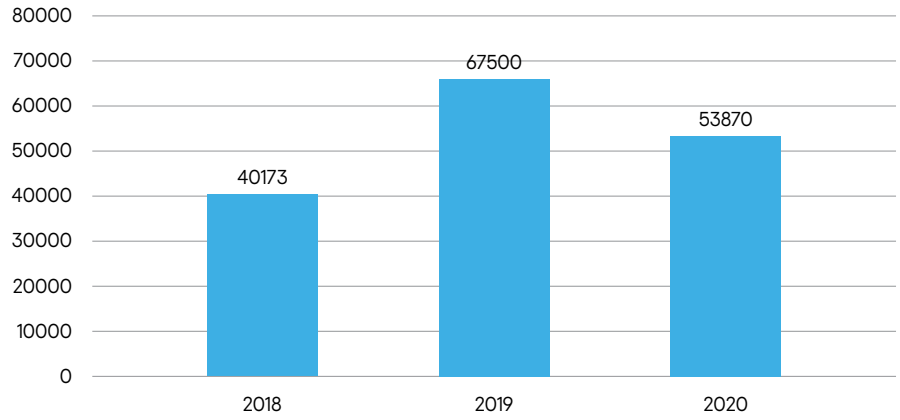


Tabela 1 Usuários individuais afetados por stalkerware globalmente de 2018 a 2020 – total por ano

Mas os números de 2020 ainda estão em um nível alto e estável. Em comparação, em 2018, houve 40.173 detecções de usuários individuais afetados globalmente por stalkerware.

Ao analisar os números do total de usuários individuais afetados por stalkerware em 2020 em todo o mundo por mês, essa tendência se torna ainda mais perceptível. Os primeiros dois meses do ano foram estáveis com muitos casos de dispositivos afetados surgindo, mostrando que o stalkerware estava bastante popular. A situação mudou em março, quando muitos países decidiram anunciar medidas de quarentena. A curva mostra uma tendência de estabilização dos números a partir de junho de 2020, quando muitos países ao redor do mundo abrandaram as restrições.

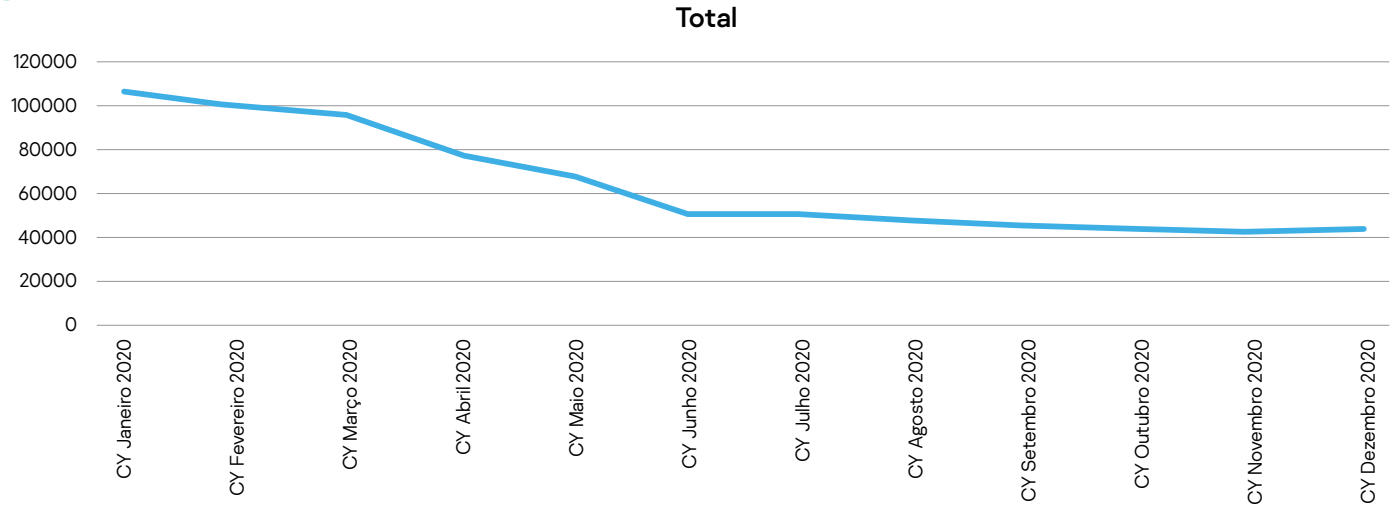


Tabela 2 Usuários individuais afetados por stalkerware em 2020 no mundo inteiro – total por ano

Mas os números de 2020 ainda estão em um nível alto e estável. Em comparação, em 2018, houve 40.173 detecções de usuários individuais afetados globalmente por stalkerware. Isso coloca em perspectiva os números totais de 2020, pois vimos uma integração crescente da tecnologia em nossas vidas. Infelizmente, isso também significa que o software usado para stalking está se tornando mais comum como outra forma de violência contra o parceiro íntimo.

Números da detecção global – amostras de stalkerware

Nesta seção, analisamos quais amostras de stalkerware são realmente as mais usadas para controlar dispositivos móveis em um nível global. Em 2020, as amostras mais detectadas podem ser vistas nos seguintes resultados:

	Amostras	Usuários afetados
1	Monitor.AndroidOS.Nicb.a	8147
2	Monitor.AndroidOS.Cerberus.s	5429
3	Monitor.AndroidOS.Agent.af	2727
4	Monitor.AndroidOS.Anlost.a	2234
5	Monitor.AndroidOS.MobileTracker.c	2161
6	Monitor.AndroidOS.PhoneSpy.b	1774
7	Monitor.AndroidOS.Agent.hb	1463
8	Monitor.AndroidOS.Cerberus.a	1310
9	Monitor.AndroidOS.Reptilic.a	1302
10	Monitor.AndroidOS.SecretCam.a	1124

Tabela 3 – As 10 amostras de stalkerware mais detectadas globalmente em 2020

1. O **Nidb** é a amostra de stalkerware mais usada em 2020, com mais de 8.100 usuários afetados globalmente. O criador do Nidb vende seu produto como Stalkerware as a Service. Isso significa que qualquer pessoa pode alugar seu aplicativo móvel e o software de servidor de controle, renomeá-lo com qualquer nome de marketing adequado e vendê-lo separadamente — exemplos disso incluem iSpyoo, TheTruthSpy, Copy9 e outros.
2. O segundo e o oitavo lugar são ocupados pela Cerberus. Essas são duas amostras diferentes da mesma família. A variante **Cerberus.a** afetou mais de 5.400 usuários.
3. O **Agent.af** ocupa o terceiro lugar, com mais de 2.700 usuários afetados. Ele é comercializado como Track My Phone e possui recursos comuns como leitura de mensagens de qualquer aplicativo, registro do histórico de chamadas de uma pessoa e rastreamento de geolocalização.
4. O **Anlost.a** é um bom exemplo de stalkerware disfarçado. Ele é divulgado como um aplicativo antifurto e seu ícone fica presente na tela inicial (comportamento incomum para aplicativos de stalkerware ocultos). Portanto, ele está disponível na Google Play Store. No entanto, é possível ocultar deliberadamente o ícone da tela inicial. Uma das principais funcionalidades do aplicativo é a interceptação de mensagens SMS e a leitura do registro de chamadas. Mais de 2.200 usuários foram afetados por essa amostra.
5. O **MobileTracker.c** tem várias funcionalidades, como intercepção de mensagens de redes sociais populares e controle remoto do dispositivo afetado. Mais de 2.100 usuários foram afetados por essa amostra.
6. O **PhoneSpy** também é conhecido como Spy Phone ou Spapp Monitoring. Esse aplicativo conta com muitos recursos de espionagem, englobando todos os aplicativos de mensagens instantâneas e redes sociais populares.
7. O **Agent.hb** é outra versão do MobileTracker. Como a versão original, ele oferece muitas funcionalidades.
8. O **Cerberus.b** é uma amostra diferente da mesma família que o Cerberus.a.
9. O **Reptilic.a** é um stalkerware que inclui muitos recursos, como monitoramento de mídias sociais, gravações de chamadas e monitoramento do histórico do navegador.
10. O **SecretCam.a** é um software de stalking por câmeras, o que significa que ele é capaz de gravar vídeos secretamente da câmera frontal ou traseira do dispositivo afetado.

Geografia dos usuários afetados

O stalkerware é um fenômeno global que afeta países independentemente de seu tamanho, sociedade ou cultura. Ao olhar para os 10 países mais afetados em 2020, as descobertas da Kaspersky mostram que, na maior parte, os mesmos países continuam sendo os mais afetados, com a Rússia em primeiro lugar. Ainda assim, vemos um aumento na atividade de stalkerware no Brasil e nos EUA em 2020 em comparação com 2019. No entanto, detectamos menos incidentes na Índia, que caiu na classificação. Também detectamos um número maior de incidentes no México, que subiu duas posições no ranking.

	País	Usuários afetados
1	Federação da Rússia	12389
2	Brasil	6523
3	Estados Unidos da América	4745
4	Índia	4627
5	México	1570
6	Alemanha	1547
7	Irã	1345
8	Itália	1144
9	Reino Unido	1009
10	Arábia Saudita	968

Tabela 4 – 10 países mais afetados por stalkerware em 2020 – globalmente

Considerando a Europa, a Alemanha, a Itália e o Reino Unido são os três países mais afetados, nessa ordem. Eles são seguidos pela França em quarto lugar e Espanha em quinto.

	País	Usuários afetados
1	Alemanha	1547
2	Itália	1144
3	Reino Unido	1009
4	França	904
5	Espanha	873
6	Polônia	444
7	Países Baixos	321
8	Romênia	222
9	Bélgica	180
10	Áustria	153

Tabela 5 – 10 países mais afetados por stalkerware em 2020 – Europa

Como verificar se um dispositivo móvel possui stalkerware instalado

É difícil para os usuários comuns saber se o stalkerware está instalado em seus dispositivos. Geralmente, esse tipo de software permanece oculto, o que inclui cultar o ícone do aplicativo stalkerware na tela inicial e no menu do telefone e até mesmo limpar quaisquer rastros deixados. No entanto, ele pode se entregar e existem alguns sinais de alerta. Entre os mais importantes estão:

- Fique atento ao esgotamento rápido da bateria, ao superaquecimento constante e ao crescimento do tráfego de dados móveis.
- Faça uma verificação antivírus regular em seu dispositivo Android: se a solução de segurança cibernética detectar stalkerware, **não se apresse para removê-lo, pois o infrator pode notar**. Tenha um plano de segurança pronto e entre em contato com uma organização de ajuda local.
- Verifique o histórico do navegador: para baixar o stalkerware, o agressor terá que visitar algumas páginas da web que o usuário afetado não conhece. Mas o histórico também pode ser apagado pelo infrator.
- Verifique as configurações de "fontes desconhecidas": Se "fontes desconhecidas" estiverem ativadas em seu dispositivo, pode ser um sinal de que um software indesejado foi instalado de uma fonte de terceiros.
- Verifique as permissões dos aplicativos instalados: o aplicativo de stalkerware pode estar disfarçado com um nome errado com acesso suspeito a mensagens, registros de chamadas, localização e outras atividades pessoais.

No entanto, também é importante compreender que os sinais ou sintomas de aviso não são necessariamente uma prova de que o stalkerware está instalado em um dispositivo.

No contexto de violência doméstica e relacionamentos abusivos, pode ser difícil ou mesmo impossível negar ao parceiro abusivo acesso ao telefone.

Como minimizar o risco

Existem alguns conselhos que podem ajudar a aumentar sua segurança digital:

- Nunca empreste seu telefone para ninguém sem ver o que acontece com o telefone e não o deixe desbloqueado.*
- Use uma senha de bloqueio de tela complexa e altere as senhas regularmente.
- Não revele sua senha a ninguém – nem mesmo a seu parceiro, familiares ou amigos próximos.*
- Faça verificações regulares em seu telefone— exclua aplicativos que você não usa e analise as permissões concedidas a cada aplicativo.
- Desative a opção de instalação de aplicativos de terceiros em dispositivos Android.
- Proteja seus dispositivos Android com uma solução de segurança cibernética, como Kaspersky Internet Security para Android (gratuita), que detecta stalkerware e emite avisos.

*No contexto de violência doméstica e relacionamentos abusivos, pode ser difícil ou mesmo impossível negar ao parceiro abusivo acesso ao telefone.

Atividades e contribuição da Kaspersky para acabar com a violência cibernética

A Kaspersky está trabalhando ativamente para acabar com a violência cibernética e stalkerware, como uma empresa e junto com muitos outros parceiros. Em 2019, criamos um alerta especial que notifica os usuários quando stalkerware é instalado em seus telefones. No mesmo ano, com outros nove membros fundadores, criamos o Coalition Against Stalkerware. Em 2020, criamos o TinyCheck, uma ferramenta gratuita para detectar stalkerware em dispositivos móveis – especificamente para organizações de serviço que trabalham com vítimas de violência doméstica. O TinyCheck pode ser encontrado em https://github.com/KasperskyLab/TinyCheck. Desde 2021, somos um dos cinco parceiros em um projeto de toda a UE que visa combater a violência cibernética e o stalkerware com base no gênero, denominado DeStalk, que a Comissão Europeia escolheu apoiar com seu Programa de Direitos, Igualdade e Cidadania.

Sobre a Coalition Against Stalkerware

A Coalition Against Stalkerware ("CAS" ou "Coalition") é um grupo dedicado a lidar com abuso, stalking e assédio por meio da criação e uso de stalkerware. Lançada em novembro de 2019, a Coalition Against Stalkerware ganhou 26 parceiros em seu primeiro ano. Isso inclui os sócios fundadores – Avira, Electronic Frontier Foundation, Rede Europeia para o Trabalho com Autores de Violência Doméstica, G DATA Cyber Defense, Kaspersky, Malwarebytes, The National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape e WEISSER RING. A CAS busca reunir uma gama diversificada de organizações para abordar ativamente comportamentos criminosos realizados por meio de stalkerware e aumentar a conscientização pública sobre esse importante problema. Devido à alta relevância social para usuários em todo o mundo e novas variantes de stalkerware surgindo periodicamente, a Coalition Against Stalkerware está aberta a novos parceiros e pede cooperação. Para saber mais sobre a Coalition Against Stalkerware, visite a página oficial https://stopstalkerware.org/pt.