O cenário do **stalkerware** em 2022

Coalition Against Stalkerware

kaspersky

Conteúdo

Principais resultados de 2022

O cenário do stalkerware é um relatório anual da Kaspersky que visa contribuir para a melhor compreensão da quantidade de pessoas afetadas pela perseguição digital no mundo. O stalkerware é um programa comercializado de maneira oficial, porém ele se mantém escondido nos celulares, permitindo com que a pessoa que o instalou monitore a vida privada de um indivíduo sem seu conhecimento.

O stalkerware pode ser baixado e facilmente instalado por qualquer pessoa com conexão à Internet e acesso físico a um smartphone. Um invasor viola a privacidade da vítima, pois pode usar o programa para monitorar grandes volumes de dados pessoais. Dependendo do tipo de software, é possível descobrir a localização do dispositivo, rastrear mensagens de texto, chats em redes sociais, fotos, histórico do navegador e muito mais. O stalkerware funciona escondido (em segundo plano), o que significa que as vítimas não sabem que todas suas ações estão sendo rastreadas.

Na maioria dos países, o uso do stalkerware não é proibido, mas instalar aplicativos desse tipo no smartphone de outra pessoa sem o seu consentimento é ilegal e passível de punição. No entanto, é o invasor que será responsabilizado, não o desenvolvedor do aplicativo.

Juntamente com outras tecnologias, o stalkerware faz parte do abuso habilitado pela tecnologia e é frequentemente usado em relacionamentos abusivos. Como isso faz parte de um problema mais amplo, a Kaspersky está trabalhando com especialistas e organizações relevantes no combate à violência doméstica, serviços de apoio às vítimas e programas de invasores por meio de pesquisas e agências governamentais para compartilhar conhecimento e fornecer apoio a profissionais e vítimas.

Destaques dos dados de 2022

- **Em 2022, os dados da Kaspersky mostram que 29.312 indivíduos únicos foram afetados pelo stalkerware em todo o mundo.** A quantidade é semelhante ao número total de usuários afetados em 2021. Levando em consideração os desenvolvimentos no software de perseguição digital nos últimos anos, os dados sugerem que há uma tendência de estabilização. De forma mais ampla, é importante observar que os dados abrangem o número afetado de usuários da Kaspersky, sendo o número global de indivíduos afetados provavelmente maior. Algumas vítimas podem usar outra solução de segurança em seus dispositivos, enquanto outros não usam nenhum programa.
- **Além disso, os dados revelam uma proliferação estável do stalkerware ao longo dos 12 meses de 2022.** Em média, 3.333 pessoas foram afetadas por stalkerware por mês. A taxa de detecção estável indica que a perseguição digital se tornou um problema persistente que merece uma atenção mais ampla da sociedade. Membros da Coalition Against Stalkerware estimam que poderia haver perto de um milhão de vítimas afetadas por stalkerware a cada ano no mundo inteiro.
- De acordo com dados da Kaspersky Security Network, o **stalkerware é mais usado na Rússia, no Brasil e na Índia,** mas continua sendo um fenômeno global que afeta todos os países. A nível regional, os dados revelam que o maior número de vítimas está localizado nos seguintes países:
  - Alemanha, Itália e França (Europa);
  - Irã, Turquia e Arábia Saudita (Oriente Médio e África);
  - Índia, Indonésia e Austrália (Ásia-Pacífico);
  - Brasil, México e Equador (América Latina);
  - Estados Unidos (América do Norte);
  - Federação Russa, Cazaquistão e Belarus (Europa Oriental (exceto países da União Europeia), Rússia e Ásia Central).
- Globalmente, o aplicativo de stalkerware mais utilizado é o Reptilicus com 4.065 afetados usuários.

Tendências de 2022 observadas pela Kaspersky

Em 2022, um total de 29.312 indivíduos únicos foram afetados por stalkerware

Números globais de detecção: pessoas afetadas

Esta seção compara as estatísticas globais e regionais coletadas pela Kaspersky em 2022 com as estatísticas dos anos anteriores. No ano passado, 29.312 indivíduos únicos foram afetados por stalkerware. O Gráfico 1 mostra a evolução das pessoas afetadas ano a ano desde 2018.

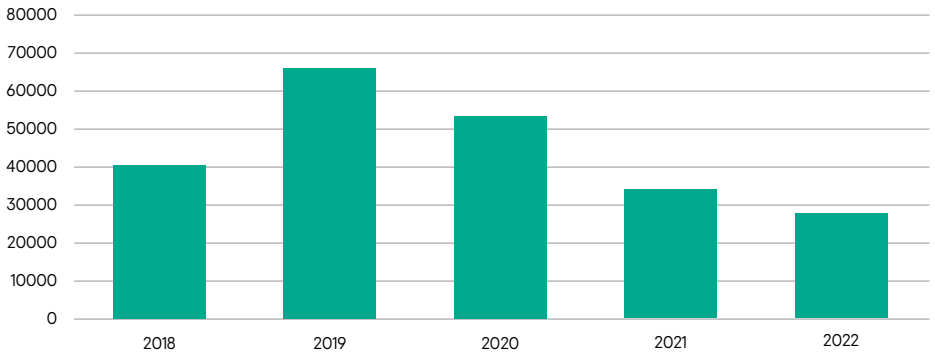


Gráfico 1 – Evolução dos indivíduos afetados ano a ano desde 2018

O Gráfico 2 abaixo mostra o número de usuários únicos afetados por mês entre 2021 e 2022. Vale ressaltar que, em 2022, a situação é quase idêntica ao ano anterior, indicando que a taxa de proliferação de stalkerware se estabilizou. Em média, 3.333 pessoas foram afetadas por stalkerware por mês.

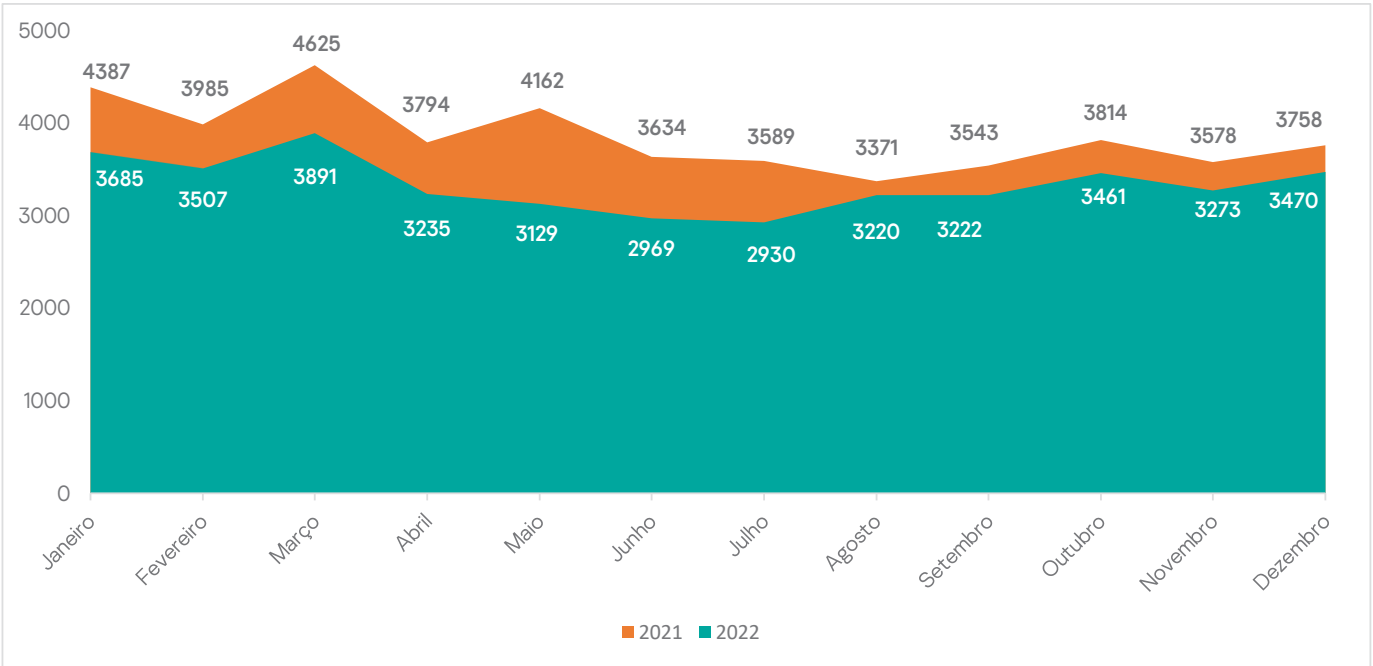
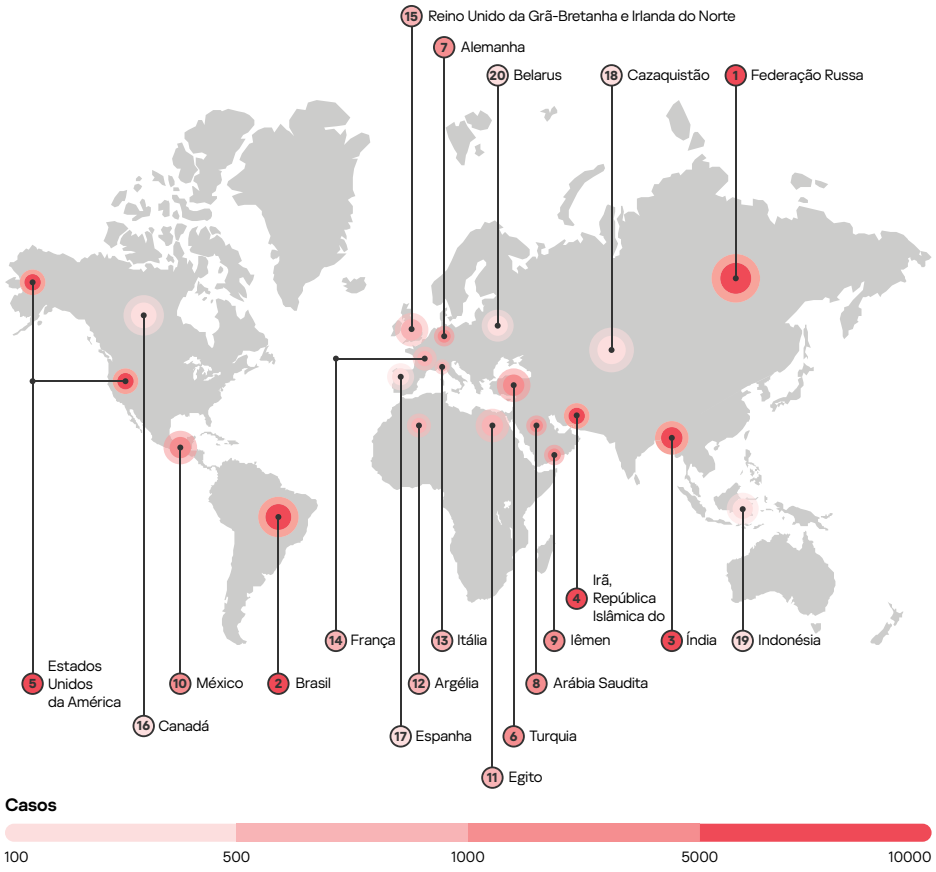


Gráfico 2 – Indivíduos afetados por mês no período de 2021 – 2022

Números globais e regionais de detecção: geografia dos usuários afetados

O stalkerware continua a ser um problema global. Em 2022, a Kaspersky detectou vítimas em 176 países.



Mapa 1 – Países mais afetados pelo stalkerware em 2022

Metodologia

Os dados deste relatório foram extraídos dos registros de detecção da rede de proteção Kaspersky Security Network (KSN). Essa rede processa todos os dados de segurança dos milhões de voluntários ao redor do mundo que decidiram participar dela. Todas as informações do sistema são anonimizadas.

Para calcular as estatísticas, foram filtrados os registros feitos pelas soluções para plataforma móveis da Kaspersky da linha de consumidores finais (domésticos) que seguem os critérios de detecção de stalkerware da Coalition Against Stalkerware. Isso significa que o número de pessoas afetadas se refere apenas a vítimas de stalkerware, pois as detecções de outras ameaças, como spyware (software espião) ou outros aplicativos de monitoramento que se enquadram na classificação da Coalition, foram excluídas do relatório.

É importante ressaltar ainda que as estatísticas refletem a quantidade de donos(as) de dispositivos móveis únicos afetados por stalkerware, o que é diferente do número total de detecções. O número de detecções pode ser maior, pois é possível que tenhamos detectado diferentes tentativas de instalação do stalkerware em um mesmo dispositivo.

Por fim, as estatísticas refletem somente consumidores de dispositivos móveis que utilizam as soluções de segurança da Kaspersky. Isso exclui, portanto, aquelas pessoas que usam outra solução de segurança em seus dispositivos ou quem não usa nenhum proteção em seu celular ou tablet.

Em 2022, Rússia (8.281), Brasil (4.969) e Índia (1.807) foram os 3 principais países com mais pessoas afetadas. Esses três países permanecem na liderança desde 2019, de acordo com as estatísticas da Kaspersky. Em comparação com os anos anteriores, vale ressaltar que o número de indivíduos afetados nos EUA caiu no ranking e agora aparece em quinto lugar, com 1.295 pessoas. Por outro lado, observou-se um aumento no Irã, que avançou para o quarto lugar com 1.754 usuários.

Em comparação com 2021, apenas o Irã aparece como um novo participante entre os 5 principais países mais afetados. Os outros quatro países – Rússia, Brasil, Índia e Estados Unidos – tradicionalmente aparecem no topo da lista. Olhando para a outra metade do ranking dos top 10, Turquia, Alemanha e México permaneceram na lista em comparação com o ano passado. Os novos participantes de 2022 são a Arábia Saudita e o Iêmen.

	País	Usuários afetados
1	Federação Russa	8.281
2	Brasil	4.969
3	Índia	1.807
4	Irã	1.754
5	Estados Unidos da América	1.295
6	Turquia	755
7	Alemanha	736
8	Arábia Saudita	612
9	Iêmen	527
10	México	474

Tabela 1 – Os 10 países mais afetados por stalkerware no mundo em 2022

Na Europa, o número total de usuários únicos afetados em 2022 foi de 3.158. Os três países mais afetados são Alemanha (737), Itália (405) e França (365). Em comparação com 2021, todos eles, incluindo o sétimo lugar na lista (Países Baixos), continuam a figurar no ranking dos mais afetados da Europa. Os novos participantes da lista são Suíça, Áustria e Grécia.

	País	Usuários afetados
1	Alemanha	736
2	Itália	405
3	França	365
4	Reino Unido	313
5	Espanha	296
6	Polônia	220
7	Países Baixos	154
8	Suíça	123
9	Áustria	71
10	Grécia	70

Tabela 2 – Os 10 países mais afetados por stalkerware na Europa em 2022

Na Europa Oriental (excluindo os países da União Europeia), Rússia e Ásia Central, o número total de indivíduos únicos afetados em 2022 foi de 9.406. Os três principais países são Rússia, Cazaquistão e Belarus.

	País	Usuários afetados
1	Federação Russa	8.281
2	Cazaquistão	296
3	Belarus	267
4	Ucrânia	258
5	Azerbaijão	130
6	Uzbequistão	76
7	Moldova	34
8	Tadjiquistão	32
9	Quirguistão	31
10	Armênia	27

Tabela 3 – Os 10 principais países mais afetados por stalkerware na Europa Oriental (excluindo países da UE), Rússia e Ásia Central em 2022

Nas regiões do Oriente Médio e África, o número total de pessoas afetadas foi de 6.330, um pouco maior do que em 2021. O ranking traz o Irã, com 1.754 usuários afetados, no topo desta lista em 2022. Com 755 vítimas, a Turquia subiu para o segundo lugar na região, seguido de perto pela Arábia Saudita, com 612 afetados.

	País	Usuários afetados
1	Irã	1.754
2	Turquia	755
3	Arábia Saudita	612
4	Iêmen	527
5	Egito	469
6	Argélia	407
7	Marrocos	168
8	Emirados Árabes Unidos	155
9	África do Sul	145
10	Quênia	123

Tabela 4 – Os 10 países mais afetados por stalkerware no Oriente Médio e na África em 2022

Na região da Ásia-Pacífico, o número total de pessoas afetadas foi de 3.187. A Índia continua muito à frente dos demais países da região, com 1.807 vítimas. A Indonésia ocupa o segundo lugar (269), enquanto a Austrália é a terceira (190).

	País	Usuários afetados
1	Índia	1.807
2	Indonésia	269
3	Austrália	190
4	Filipinas	134
5	Malásia	129
6	Vietnã	109
7	Bangladesh	105
8	Japão	95
9	Tailândia	52
10	Paquistão	48

Tabela 5 – Os 10 países mais afetados por stalkerware na região Ásia-Pacífico em 2022

A região da América Latina e Caribe é dominada pelo Brasil, com 4.969 indivíduos afetados. Isso representa aproximadamente 32% do número total de vítimas da região. Em seguida estão México e Equador, enquanto a Colômbia passou para o quarto lugar. Um total de 6.170 pessoas foram afetadas na região em 2022.

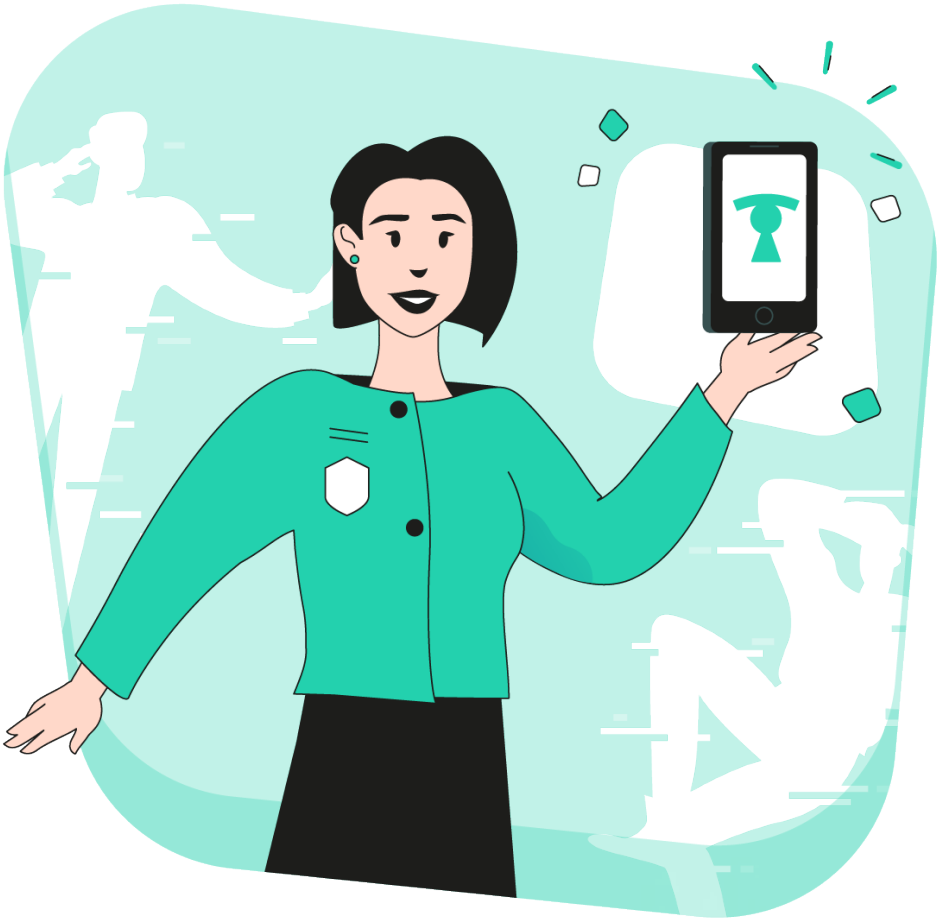
	País	Usuários afetados
1	Brasil	4.969
2	México	474
3	Equador	146
4	Colômbia	120
5	Peru	111
6	Argentina	85
7	Chile	49
8	Bolívia	32
9	Venezuela	30
10	República Dominicana	24

Tabela 6 – Os 10 países mais afetados por stalkerware na América Latina em 2022

Finalmente, na América do Norte, 87% de todos os usuários afetados estão nos Estados Unidos. Isso é esperado, considerando o tamanho relativo da população americana em comparação com o Canadá. Nessa região foram registradas 1.585 vítimas.

	País	Usuários afetados
1	Estados Unidos da América	1.295
2	Canadá	299

Tabela 7 – Número de usuários afetados por stalkerware na América do Norte em 2022



Os dispositivos com os sistemas Android e iOS são igualmente afetados pelo stalkerware?

Os programas stalkerware são menos frequentes nos iPhones em comparação com os dispositivos Android porque o iOS é um sistema fechado. No entanto, os invasores podem contornar essa limitação em iPhones com o jailbreak, mas ainda precisam ter o acesso físico ao telefone para fazê-lo. Os proprietários de iPhone que temem a vigilância devem sempre ficar de olho em seus dispositivos.

Uma outra possibilidade é o agressor oferecer à vítima um iPhone – ou qualquer outro dispositivo – com o stalkerware já instalado. Existem muitas empresas que oferecem esse serviço, permitindo que os abusadores tenham essas ferramentas instaladas em novos telefones, os quais podem ser entregues em embalagens de fábrica sob o disfarce de um presente para a vítima.

Números globais de detecção: aplicativos stalkerware

Esta seção lista os aplicativos stalkerware mais comuns encontrados nos smartphones ao redor do mundo. Em 2022, o app mais popular foi o Reptilicus (4.065 usuários afetados) e a Kaspersky detectou um total de 182 stalkerware diferentes.

	Nome do aplicativo	Usuários afetados
1	Reptilicus (também conhecido como Vkurse)	4.065
2	Cerberus	2.407
3	KeyLog	1.721
4	MobileTracker	1.633
5	wSpy	1.342
6	SpyPhone	1.211
7	Anlost	1.189
8	Track My Phones	1.137
9	MonitorMinor	864
10	Hovermon	827

Tabela 8 – Lista dos 10 principais aplicativos de stalkerware em 2022

O stalkerware fornece um meio de controlar a vida da vítima e seus recursos variam dependendo do aplicativo, e se ele foi pago ou baixado gratuitamente. Em geral, esse tipo de programa usa um disfarce de ferramentas antifurto ou de controle parental, mas, na realidade, sua operação são distintas das ferramentas legítimas. As principais diferenças são que os stalkerware são instalados sem a permissão ou aviso da pessoa que será monitorada, além do programa rodar furtivamente (escondido) no dispositivo da vítima.

Abaixo estão algumas das funções mais comuns nos aplicativos stalkerware:

- Ocultação do app (ícone na tela inicial)
- Leitura de mensagens SMS, MMS e registro de chamadas
- Acesso a listas de contatos
- Rastreamento da localização via GPS
- Acesso aos eventos do calendário
- Leitura de mensagens em app de mensagens 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.
- Visualização de fotos e imagens das galerias
- Captura de telas
- Captura de fotos com a câmera frontal (modo de selfie)

Perseguição digital e violência de gênero

Stalkerware é um método de perseguição online que faz parte da violência digital

Tanto mulheres quanto homens podem ser vítimas de violência digital, mas pesquisas mostram que na esmagadora maioria dos casos, as mulheres são o principal alvo por causa de seu gênero. É importante lembrar que a violência digital é uma outra dimensão da violência. Ela precisa ser entendida como um continuação da violência offline, pois tem efeitos reais e negativos sobre as vítimas. Para obter mais informações, leia o documento "Violência Cibernética contra Mulheres e Meninas: Principais Termos e Conceitos" (2022) publicada pelo Instituto Europeu para a Igualdade de Gênero.

A importância dos dados para entender o escopo da violência digital – Dra. Leonie Maria Tanczer, professora associada da University College London e chefe do Grupo de Pesquisa de Gênero e Tecnologia da UCL

Pesquisas anteriores sobre formas de stalking e violência de gênero impulsionadas pela tecnologia se concentraram em uma série de sistemas digitais rotineiros que podem coagir, controlar e prejudicar uma pessoa ou grupos de indivíduos. Embora o relatório e os dados atuais sejam restritos a dispositivos móveis, a perseguição digital pode ser facilitada por meio de vários dispositivos, incluindo rastreadores GPS ou a chamada "Internet das Coisas" (IoT). Este último inclui produtos inteligentes e habilitados para a Internet, como campainhas inteligentes, câmeras de CFTV ou alto-falantes.

As evidências baseadas em abuso por tecnologia ainda são restritas. Os centros de pesquisa atuais são predominantes na Austrália, Reino Unido e EUA. A maioria dos estudos está, consequentemente, focada em dados provenientes desses países, o que cria pontos cegos. Dados como os oferecidos neste relatório contribuem para uma compreensão mais ampla do cenário de abuso habilitado para tecnologia, que é urgentemente necessária.

Os serviços de apoio às vítimas também demonstraram ter dificuldades com os crescentes requisitos para se manterem atualizados com os desenvolvimentos tecnológicos. Eles pediram complementos para as práticas existentes de avaliação de risco e segurança, incluindo "planos de ação de cyberstalking" e treinamento dedicado para aumentar as habilidades e a capacidade de resposta do setor. De fato, ofertas de serviços cada vez mais especializadas estão sendo disponibilizadas, como mostra a equipe de Segurança Técnica de Refúgio (Refuge's Tech Safety team), o Projeto de Rede de Segurança da Rede Nacional para Acabar com a Violência Doméstica (Safety Net Project by the National Network to End Domestic Violence, NNEDV) ou a Clínica para Acabar com o Abuso de Tecnologia (Clinic to End Tech Abuse, CETA).

O Grupo de Pesquisa de Gênero e Tecnologia da University College London (UCL) investiga os pontos de interseção de tecnologia, segurança e gênero para fazer com que os sistemas digitais funcionem para todos. Saiba mais:

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

Preste mais atenção ao sofrimento da violência digital – Elena Gajotto, vice-presidente da Una Casa Per L'Uomo

Cyberstalking tem um impacto concreto na realidade daqueles que sofrem com isso. Existem efeitos psicológicos, físicos e sociais de médio a longo prazo que vemos diariamente em nossos centros antiviolência. Como o Serviço de Pesquisa do Parlamento Europeu sublinhou em seu estudo (2021), todas as mulheres podem ser potenciais vítimas de cyberstalking, sejam elas figuras públicas, ex-parceiras ou simplesmente utilizadoras de mídias sociais. O cyberstalking engloba diferentes tipos de comportamentos, como mensagens persistentes, monitoramento da atividade de uma vítima ou outras formas de busca on-line e, como afirma o mesmo estudo, "pode ser que o cyberstalking seja simplesmente uma ferramenta adicional no kit de ferramentas do stalker".

Ao trabalhar a violência digital, as seguintes características precisam ser consideradas:

- A violência digital pode ser realizada juntamente com outras formas de violência (física, sexual, psicológica, econômica etc.).
- A violência pode começar on-line e depois continuar off-line, ou, vice-versa
- Não é simples remover - permanentemente - conteúdos ofensivos, violentos ou desencadeantes publicados online.
- Os autores da violência digital podem ser indivíduos ou grupos, e podem ser conhecidos e desconhecidos para a vítima.
- A violência digital pode ser realizada por meio de uma ampla gama de dispositivos (PCs, smartphones, dispositivos domésticos inteligentes etc.) e em muitas plataformas diferentes (sites, aplicativos de mensagens, bate-papos on-line, mídias sociais etc.).

Como mencionado acima, apesar de serem realizadas na esfera cibernética, essas formas de violência têm um impacto profundo e tangível na realidade das vítimas. Estudos mostram que as mulheres são as principais vítimas de cyberstalking ou outras formas de violência digital. Elas experimentam muitos dos mesmos sintomas das vítimas de violência off-line, como, por exemplo, ansiedade, ataques de pânico, TEPT, pensamentos suicidas, raiva, falta de autoconfiança e dificuldades de concentração. Pode haver também efeitos econômicos negativos (extorsão, perda de renda etc.) e relacionais (perda de rede familiar e de amigos, isolamento social etc.). Além disso, a violência digital também tem um impacto coletivo, tanto a nível econômico como político, com um aumento dos custos jurídicos, administrativos e de saúde públicos por um lado, e uma menor participação das mulheres no discurso público.

Una Casa Per L'Uomo é uma organização da sociedade civil italiana que gere serviços de apoio às vítimas. A Una Casa Per L'Uomo foi parceira do consórcio do projeto DeStalk (2021-2023), cofinanciado pelo Programa de Direitos, Igualdade e Cidadania da União Europeia, e é membro da Coligação Contra o Stalkerware.

Portanto, é importante enfatizar o perigo desse fenômeno. A sociedade precisa prestar mais atenção ao sofrimento da violência digital. Para lidar com o problema, estamos trabalhando com nossos membros, bem como colaboramos com a Kaspersky e todos os parceiros da Coalition Against Stalkerware para apoiar as vítimas e treinar melhor os profissionais que trabalham no campo da violência doméstica.

Abordando atitudes sociais que apoiam o abuso facilitado pela tecnologia — Anna McKenzie, gerente de comunicações da WWP EN

O abuso impulsionado pela tecnologia, como o stalkerware, é uma preocupação crescente para nossas organizações-membros, que trabalham em mudanças comportamentais com praticantes de violência doméstica.

A violência digital continua a aumentar: dispositivos conectados, software secretos de vigilância e espaços on-line oferecem o ambiente perfeito para parceiros abusivos estenderem o controle sobre a vida de seus pares. No entanto, verificar o telefone de um parceiro, ler seus e-mails, estar ciente de sua localização e saber suas senhas é agora tão comum que os indivíduos muitas vezes nem percebem que estão exibindo comportamentos abusivos.

Como essas aparentes violações de privacidade não são percebidas como tal?

Em 2021, a Kaspersky publicou o report "Stalking online em relacionamentos", destacando algumas tendências preocupantes. De acordo com os dados, comportamentos como o de estimular as atividades digitais de um parceiro com o seu consentimento foram amplamente considerados aceitáveis para garantir a transparência dentro de um relacionamento. É preocupante, no entanto, que quase um terço dos entrevistados se sentia bem em monitorar as atividades de um parceiro sem o seu consentimento, especialmente se eles acreditavam que seu parceiro estava sendo infiel.

Essas atitudes falam diretamente de questões que os membros de nossas organizações encontram regularmente em seu trabalho com agressores de violência doméstica digital. É altamente problemático supor que uma pessoa que não consente em ter seus dispositivos vigiados implique que ela esteja escondendo uma possível infidelidade. Em relacionamentos abusivos, o consentimento é tênue na melhor das hipóteses: como eles podem dizer sim, se eles não podem dizer não, afinal? Da mesma forma, a aceitação da suspeita de infidelidade como desculpa para espionar um parceiro é uma oportunidade de ouro para parceiros abusivos que constantemente percebem uma ameaça de traição em seus relacionamentos. Isso também fala em direção a um senso de propriedade e uma falta de comunicação saudável, que são preocupações centrais em relacionamentos abusivos.

Acreditamos que, além da necessidade óbvia de regulamentação legal, capacitação e conscientização geral sobre a questão da violência digital, é de extrema importância que as atitudes de apoio ao abuso em relação à violação facilitada pela tecnologia sejam abordadas desde cedo e de maneira generalizada. Estudos como o relatório State of Stalkerware são uma verificação importante do status quo, mas temos de fazer mais para mudar o cenário. Com o #NoExcuse4Abuse, desenvolvido e implementado em cooperação com a Kaspersky, demos um primeiro passo para abordar atitudes sociais prejudiciais em relação ao abuso facilitado pela tecnologia e stalkerware.

A WDP EN é uma rede europeia com 69 membros de 34 países. Acreditamos que, sem uma abordagem para atingir os criminosos de violência doméstica e responsabilizá-los, qualquer estratégia para parar a violência por parceiro íntimo é incompleta. Nosso trabalho se concentra em deter a violência dos homens, responsabilizá-los e promover a Convenção de Istambul. Saiba mais:

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

Juntos na luta contra o stalkerware

Stalkerware não é apenas um problema técnico, é um problema que está na sociedade, portanto, requer ação de todas as suas áreas. Neste sentido, o comprometimento da Kaspersky não se limita a proteção das pessoas contra essa ameaça, mas também em manter um diálogo com organizações sem fins lucrativos, com a indústria, pesquisadores e agências públicas em todo o mundo para trabalhar juntas em soluções para esse problema.

Em 2019, a Kaspersky foi a primeira empresa de cibersegurança a desenvolver uma notificação para seus clientes para avisá-los sobre a presença de um stalkerware em seus dispositivos. Embora as soluções da Kaspersky sinalizem sobre a presença de aplicativos potencialmente nocivos que não são malware (incluindo stalkerware) há muitos anos, essa notificação deixa claro que o app tem a capacidade de espionar a vítima e que ele está no dispositivo.

Em 2022, como parte do lançamento do novo portfólio de produtos para consumidores finais da Kaspersky, o alerta de privacidade foi ampliado e agora orienta também que uma possível remoção do stalkerware irá alertar a pessoa que o instalou. Esta abordagem é importante, pois deletar o app pode levar ao agravamento da situação. Além disso, a pessoa corre o risco de apagar dados ou evidências importantes que podem ser usados como provas em um processo. A Figura 2 (abaixo) mostra o visual do aviso. O alerta de privacidade está presente em todos as soluções de segurança doméstica da Kaspersky para oferecer proteção contra o stalkerware.

Em 2019 a Kaspersky cofundou a Coalition Against Stalkerware, grupo de trabalho internacional de combate ao stalkerware e à violência doméstica que reúne empresas privadas de TI, ONGs, instituições de pesquisa e agências regulatórias que trabalham para combater o cyberstalking e ajudar vítimas de abuso online. Por meio de um consórcio de mais de 40 organizações, as partes interessadas podem compartilhar conhecimento e trabalhar juntas para resolver o problema da violência online. O site da coalizão, disponível em 7 idiomas diferentes, oferece ajuda e orientação às vítimas, caso suspeitem da presença de stalkerware em seus dispositivos.

De 2021 a 2023, a Kaspersky foi uma parceira de consórcio do projeto da UE DeStalk, cofundado pelo Programa Cidadania, Igualdade, Direitos e Valores da União Europeia. Os cinco parceiros do projeto que formaram o consórcio combinaram a experiência da comunidade de segurança de TI, pesquisa, organizações da sociedade civil e autoridades públicas. Como resultado, o projeto DeStalk treinou um total de 375 profissionais que trabalham diretamente em serviços de apoio às mulheres e programas de agressores, além de funcionários do poder público, em como enfrentar efetivamente o stalkerware e outras formas digitais de violência de gênero, além de aumentar a conscientização pública sobre violência digital e stalkerware.

Como parte do projeto, a Kaspersky desenvolveu um curso online sobre violência cibernética e stalkerware em sua Kaspersky Automated Security Awareness Platform, uma plataforma de treinamento de microaprendizado online disponível gratuitamente, que pode ser acessada em cinco idiomas diferentes. Até o momento, mais de 130 profissionais concluíram o curso, e outros 80 estão participam no momento. Embora o projeto DeStalk tenha terminado, o curso de e-learning ainda está disponível no site do projeto DeStalk https://www.work-with-perpetrators.eu/destalk.

Em junho de 2022, a Kaspersky lançou o site TinyCheck para divulgar a ferramenta de código aberto que pode ser usada por organizações sem fins lucrativos e unidades policiais para ajudar no apoio a vítimas de perseguição digital. Em 2020, a ferramenta foi criada para verificar os dispositivos em busca de stalkerware e aplicativos de monitoramento sem avisar o criminoso sobre a verificação. Ele não requer instalação no dispositivo do usuário porque funciona de forma independente para evitar a detecção por um perseguidor. O TinyCheck verifica o tráfego de saída de um dispositivo usando uma conexão Wi-Fi regular e identifica interações com fontes conhecidas, como servidores relacionados a stalkerware. O TinyCheck também pode ser usado para verificar qualquer dispositivo em qualquer plataforma, incluindo iOS, Android ou qualquer outro sistema operacional.

Você acha que é uma vítima de stalkerware? Aqui estão algumas dicas...

Quer você seja ou não uma vítima de stalkerware, aqui estão algumas dicas para se proteger melhor:

- Proteja seu telefone com uma senha forte e nunca compartilhe esse código com seu parceiro, amigos ou colegas.
- Altere as senhas de todas as suas contas periodicamente e não as compartilhe com ninguém.
- Baixe aplicativos apenas de fontes oficiais, como Google Play ou Apple App Store.
- Instale uma solução de segurança de TI confiável, como o Kaspersky for Android, nos dispositivos e examine-os regularmente. No entanto, no caso de stalkerware potencialmente 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 perpetrador será notificado se a vítima fizer uma varredura no dispositivo ou remover um aplicativo de stalkerware. Se isso acontecer, poderá causar o agravamento da situação e mais agressões. É por isso que é importante proceder com cautela se você acha que está sendo alvo de stalkerware.

- **Entre em contato com uma organização de apoio local:** para encontrar uma perto de você, consulte o site da Coalition Against Stalkerware.
- **Fique atento aos seguintes sinais de alerta:** eles podem incluir uma bateria descarregando rapidamente devido a aplicativos desconhecidos ou suspeitos consumindo sua carga, bem como 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 ativada, isso pode ser um sinal de que um software indesejado foi instalado de uma fonte externa. No entanto, os indicadores acima são circunstanciais e não indicam a presença inequívoca de stalkerware no dispositivo.
- **Não tente apagar o stalkerware, nem altere nenhuma configuração ou adultere seu telefone:** isso pode alertar seu potencial invasor e levar a ao agravamento da situação. E você ainda correrá o risco de apagar dados ou evidências importantes que poderiam ser usados em um processo.

Para obter mais informações sobre nossas atividades em stalkerware ou qualquer outra solicitação, escreva 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.

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

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

TinyCheck: https://tiny-check.com

www.kaspersky.com.br

© 2023 AO Kaspersky Lab. As marcas registradas e marcas de serviço são de propriedade de seus respectivos proprietários

Coalition Against Stalkerware

TinyCheck®

kaspersky