O Estado do **Stalkerware** em 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST STALKERWARE

Sobre a Coalition Against Stalkerware

É um novo grupo global que combina especialistas para dar suporte e ajuda em cibersegurança para vítimas de stalkerware

Em 29 de nobembro, dez organizações – Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA CyberDefense, Kaspersky, Malwarebytes, Rede Nacional pelo Fim da Violência Doméstica, NortonLifeLock, Operation Safe Escape e WEISSER RING – lançaram a iniciativa global Coalition Against Stalkerware (Coalizão contra o Stalkerware) para proteger usuários contra os programas de espionagem.

Ela nasceu para facilitar a comunicação entre a comunidade de segurança e as organizações que trabalham para combater a violência doméstica. Com o lançamento do portal www.stopstalkerware.org, a coalição tem como objetivo ajudar as vítimas, facilitando a troca de conhecimento entre os membros, desenvolvendo boas práticas para o desenvolvimento ético de software e orientando o público sobre os perigos do stalkerware.

O projeto foi criado como uma iniciativa sem fins lucrativas para reunir ONGs, indústria e organizações de outras áreas, como autoridades legais, em volta desta causa. Devido à grande relevância social para usuários em todo o mundo, com novas variações de stalkerware sendo desenvolvidas regularmente, a Coalition Against Stalkerware está aberta a novos parceiros e busca cooperação.

Para mais informações, acesse www.stopstalkerware.org

O que dizem os fundadores sobre a relevância de **trabalharem juntos contra o stalkerware**:

COALITION AGAINST STALKERWARE

Alexander Vukcevic,
Diretor do laboratório de proteção, **Avira**

"O software de monitoramento evoluiu rapidamente nos últimos anos, funções poderosas de vigilância foram adicionadas e a finalidade de rastreamento de atividades mudou de forma fundamental. O aumento contínuo no uso de dispositivos móveis, combinado à falta de mitigação legislativa, está oferecendo ferramentas acessíveis a pessoas para espionar cônjuges, familiares ou amigos. A Avira reconhece que essa é uma nova categoria de ameaças e convida empresas de segurança de TI e organizações que trabalham contra a violência doméstica a unirem forças, compartilhar informações e trabalharem juntas para acabar com essas violações de privacidade."

Eva Galperin,
Diretor de segurança cibernética, **Electronic Frontier Foundation**

"O stalkerware, usado para espionar telefones e computadores em situações de assédio ou abuso doméstico, é um problema seríssimo e muitas vezes caminha lado a lado com outras formas de abuso, incluindo a violência física. O surto de stalkerware é um problema complexo e precisamos envolver oganizações de todos os setores da sociedade para combatê-lo com eficiência."

Anna McKenzie, Gerente de comunicações, **European Network for the Work with Perpetrators of Domestic Violence (WWP EN)**

"Estudos demonstraram que 70% das mulheres vítimas de espionagem cibernética também sofreram, no mínimo, uma forma de violência física e/ou sexual de seu parceiro íntimo. Precisamos impedir que esses criminosos usem os telefones de suas parceiras para espioná-las e ainda as responsabilizem pela violência que cometem. A Coalition Against Stalkerware nos permite compartilhar nosso conhecimento sobre os agressores e a violência de gênero com empresas de segurança de TI – para que possamos trabalhar juntos e acabar com a violência contra mulheres e meninas realizadas por meio das das novas tecnologias."

Hauke Gierow,
Porta-voz para assuntos de imprensa, **G DATA CyberDefense**

"Instalar spyware no telefone de um cônjuge é uma violação de direitos humanos fundamentais. Estamos determinados a combater esse comportamento e a proteger sobreviventes de comportamento abusivo, especialmente mulheres. A G DATA Cyber Defense tem o compromisso de informar usuários sobre os possíveis riscos, além de trabalhar com organizações de apoio às vítimas para também encarar as questões não técnicas associadas ao stalkerware."

Vyacheslav Zakorzhevsky,
Chefe de pesquisa anti-malware, **Kaspersky**

"Para conter esse problema, é importante que fornecedores de soluções de cibersegurança e organizações de defesa unam forças. A indústria de segurança de TI participa melhorando a detecção de stalkerware e ao notificar os usuários desta ameaça à sua privacidade. As organizações de apoio e defesa trabalham diretamente com vítimas de violência doméstica, conhecem suas dificuldades e necessidades e podem ajudar a nortear o nosso trabalho. Dessa forma, ao agir juntos, poderemos ajudar vítimas através de expertise técnica e desenvolvimento de capacidade."

David Ruiz,
Escritor sobre privacidade on-line, **Malwarebytes Labs**

"Há anos a Malwarebytes percebeu e alerta usuários sobre os perigos potenciais do stalkerware, uma ameaça invasiva que pode acabar com a expectativa e o direito de privacidade dos indivíduos. Assim como o abuso que ele pode possibilitar, o stalkerware também se prolifera fora da visão do público, deixando vítimas e sobreviventes isolados, sem voz e indefesos. A união e a luta com a Coalition Against Stalkerware são o próximo passo, uma medida necessária para combater essa ameaça digital: uma abordagem colaborativa pautada pela promessa de possibilitar o uso de tecnologia para todos em todos os lugares."

Erica Olsen,
Diretora do projeto de rede de segurança, **Rede Nacional pelo Fim da Violência Doméstica**

"Quando projetado para operar no modo totalmente furtivo, sem notificação persistente para o proprietário do dispositivo, o stalkerware pode proporcionar aos instaladores, chamados stalkers, e outros criminosos uma ferramenta robusta para cometer assédio, monitorar, espionar e abusar. Esse tipo de abuso pode aterrorizar, traumatizar e levanta considerações importantes de privacidade e segurança. A criação da Coalizão é um avanço importante para combater o problema."

Kevin Roundy,
Diretor de pesquisa, **NortonLifeLock**

"Na NortonLifeLock, nossos especialistas em pesquisa trabalham duro para tirar o stalkerware das mãos de criminosos há mais de 12 anos, oferecendo às vítimas e possíveis vítimas ferramentas para ajudar a se protegerem e viverem livre de assédio, violência e ataques. Temos orgulho de fazer parte da fundação da Coalition Against Stalkerware para compartilhar nossa expertise e unir forças na luta contra o abuso."

Wilson "Chilly" Hightower,
Chefe de admissões, **Operation Safe Escape**

"A existência nociva do stalkerware só serve para violar, prejudicar e causar uma sensação constante de medo e ansiedade em muitos de nossos clientes. Essa é uma ameaça ativa e existencial para a segurança e privacidade de todas as pessoas. Assim como nossas vidas se tornam mais enraizadas e dependentes da tecnologia, a ameaça que o stalkerware representa já cresce em sua ordem de grandeza. É mais importante do que nunca se antecipar a este tipo de ameaça para tirar o poder de possíveis criminosos, stalkers e outras entidades maliciosas. A Operation Safe Escape tem um orgulho enorme de fazer parte desse esforço em grupo para restaurar a privacidade e a segurança para nossos clientes e profissionais em todos os lugares."

Horst Hinger,
Diretor-adjunto de gestão, **WEISSER RING**

"Como uma organização sem fins lucrativos, sabemos que a tecnologia facilita o acesso de criminosos aos dados privados de suas vítimas. As vítimas raramente buscam ajuda porque se sentem envergonhadas. Para a WEISSER RING, a espionagem é um problema cada vez mais importante com o qual nos deparamos ao ajudar nossas vítimas. Em 2018, atuamos em 1.019 casos de espionagem, um aumento de cerca de 3% em relação ao ano anterior. De acordo com estatísticas da polícia alemã, em 2018 foram quase 19.000 casos de espionagem, um aumento de quase 500 em relação ao ano anterior: outro claro aumento. É por isso que desenvolvemos o aplicativo NO STALK em conjunto com a WEISSER RING Foundation para proporcionar às vítimas uma ferramenta efetiva para documentar as provas da espionagem."

Principais descobertas, atualizado em abril de 2020

No mundo inteiro, o número de usuários com stalkerware instalado em seus dispositivos aumentou em 67% em apenas um ano

Esta seção fornece uma atualização com números para todo o ano de 2019 em comparação a 2018. Devido à data de publicação, o restante do relatório contém dados de janeiro a agosto de 2019.

- Ao final de 2019, o número de nossos usuários de dispositivos móveis que enfrentaram stalkerware aumentou em 67%: 40.386 usuários diferentes foram atacados em 2018; em 2019 esse número aumentou para 67.500
- Houve um aumento duas vezes maior no número de ataques na segunda metade de 2019 em comparação à primeira metade do ano. Em janeiro de 2019, 4.483 usuários de dispositivos móveis com produtos Kaspersky sofreram ataques; em setembro de 2019, esse número aumentou para 9.546. Em dezembro do mesmo ano, o número de usuários atacados chegou a 11.052.
- Rússia, Brasil, Índia e EUA são as regiões mais proeminentes para ação de stalkerware no mundo inteiro, sendo responsáveis por 23.4%, 9.4%, 9% e 5.6% dos usuários afetados em 2019, respectivamente.
- Quanto à Europa, Alemanha (3.1%), Itália (2.4%) e França (1.8%) são as três regiões com mais casos, respectivamente

Sumário

Stalkerware permite que um criminoso vigie e espione uma vítima sem o seu consentimento

Introdução e metodologia

Há seis meses, criamos um alerta especial para notificar os usuários sobre produtos de spyware comerciais (stalkerware) instalados em seus telefones. Esse relatório examina o uso de stalkerware e o número de usuários afetados por esse tipo de software nos primeiros oito meses de 2019.

A tecnologia de vigilância do consumidor evoluiu rapidamente ao longo dos últimos anos, e a própria finalidade da atividade de vigilância mudou drasticamente. A ascensão da Internet e a subsequente explosão do uso de dispositivos móveis levaram ao surgimento de um tipo de software de vigilância conhecido como stalkerware. O software permite que os usuários espionem outras pessoas, por exemplo, para monitorar suas mensagens, informações de chamadas e localizações de GPS, de forma completamente invisível. Ele é frequentemente usado para invadir a privacidade de parceiros e ex-parceiros e até mesmo de estranhos. Basta instalar manualmente um aplicativo no smartphone ou tablet da vítima. Após a instalação, o invasor terá acesso a diversos dados pessoais, independentemente de estar longe da vítima. Ele é bastante diferente de software de controle dos pais. Enquanto os apps de controle dos pais visam restringir acesso a conteúdo arriscado e impróprio e notificam um usuário sobre suas solicitações, o stalkerware permite que o invasor vigie e espione uma vítima sem que ela autorize.

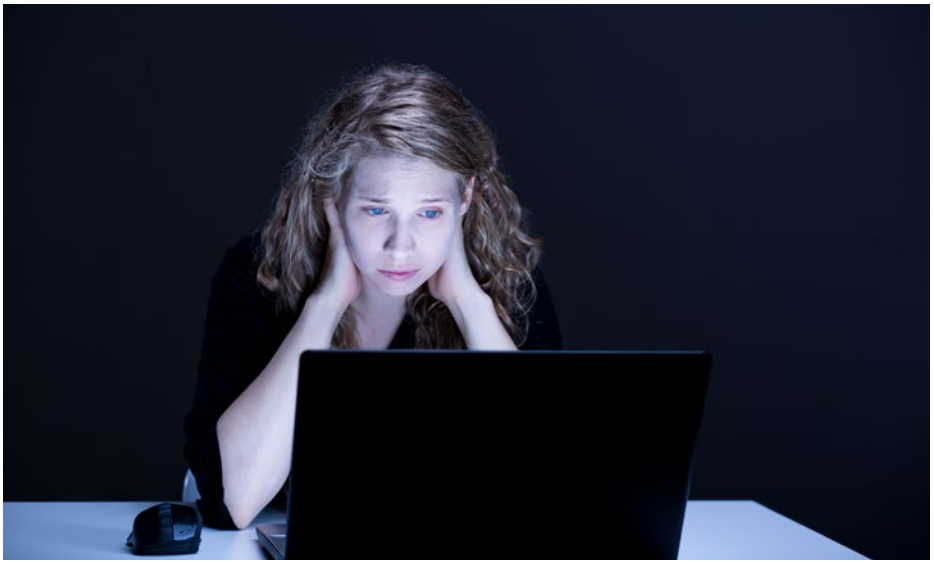
A grande maioria dos apps de stalkerware não está disponível nas lojas de apps oficiais, como Google Play, e a instalação requer acesso a um site dedicado e ao dispositivo da vítima. Pessoas mal-intencionadas podem usá-los para monitorar emails de funcionários, rastrear deslocamentos de crianças e até mesmo espionar o que um parceiro está fazendo. Essas utilizações podem levar a assédios, vigilância sem consentimento, stalking e até mesmo violência doméstica.
No entanto, as leis atuais para regular o uso de stalkerware ainda não são rigorosas o suficiente para dissuadir os responsáveis por abusar e se aproveitar de outras pessoas.

Os dados neste relatório foram obtidos de estatísticas de ameaças agregadas da Kaspersky Security Network para medir a frequência e a quantidade de usuários que enfrentaram ameaças de stalkerware nos primeiros oito meses de 2019 em comparação ao que foi encontrado no último ano. A Kaspersky Security Network é a infraestrutura dedicada a processar streams de dados relacionados à segurança cibernética de milhões de participantes voluntários ao redor do mundo. Nesse relatório, exploramos o motivo pelo qual stalkerware está sendo usado e onde ele é implementado de forma mais prolífica.

Principais descobertas

Globalmente, a quantidade de usuários com stalkerware instalado em seus dispositivos aumentou em 35% em apenas um ano

- No mundo, de janeiro a agosto de 2019, houve mais de 518.223 casos em que as nossas tecnologias de proteção registraram a presença de stalkerware em dispositivos de usuários ou detectaram uma tentativa de instalá-lo, um aumento de 373% em relação ao mesmo período de 2018
- Nos primeiros oito meses de 2019, 37.532 usuários encontraram stalkerware pelo menos uma vez. Isso representa um aumento de 35% em relação ao mesmo período de 2018 quando 27.798 usuários foram alvos
- O número de usuários para os quais spyware agressivo foi detectado como Trojan Spy atingiu 26.620 nos primeiros oito meses de 2019, uma minoria se comparado ao número de usuários que encontraram stalkerware
- No mundo, a Federação Russa permanece a região mais proeminente para stalkerware, contabilizando 25,6% dos possíveis usuários afetados nos primeiros oito meses de 2019. A Índia é o segundo lugar, com 10,6% de usuários afetados, e o Brasil está em terceiro lugar (10,4%). Os Estados Unidos estão em quarto, com 7,1%.
- Quanto à Europa, Alemanha, Itália e Reino Unido são as três regiões com mais casos, respectivamente



Aumento da incidência de stalkerware

Neste ano, houve um aumento abrupto das detecções de stalkerware em dispositivos Android protegidos por produtos Kaspersky. Um motivo para esse aumento poderia ser a melhoria da detecção de stalkerware pelas soluções de segurança cibernética. Em abril, a Kaspersky lançou um recurso em seu app de segurança para Android, o Privacy Alert, que, especificamente, alerta os usuários caso um software que pode ser usado para stalking seja encontrado no dispositivo. Desde então, o número de detecções tem aumentado constantemente. Por exemplo, 4.315 usuários encontraram stalkerware em março de 2019, comparados a 7.075 em abril, um aumento de 64% em apenas um mês. Esse número aumentou para 9.251 durante agosto, 94% mais alto que no mês anterior ao lançamento da funcionalidade.

Esses programas de vigilância vendidos abertamente para consumidores são frequentemente usados para espionar colegas, parentes ou parceiros, e estão sendo muito procurados. Por um preço relativamente modesto, às vezes, tão baixo quanto US$ 7 ao mês, esses apps permanecem ocultos enquanto mantêm seus operadores informados sobre a atividade do dispositivo, como a localização de seu proprietário, histórico do navegador, mensagens de texto, conversas em redes sociais e muito mais. Alguns deles podem até mesmo gravar vídeos e voz.

Para examinar ainda mais a extensão do problema de stalkerware, a Kaspersky analisou os últimos oito meses de atividade. De janeiro a agosto de 2019, 37.533 usuários encontraram stalkerware em seus dispositivos pelo menos uma vez. Isso representa um aumento de 35% em relação ao mesmo período de 2018, quando 27.798 usuários foram alvos. No geral, houve 518.223 casos em que produtos Kaspersky registraram a presença de stalkerware em dispositivos de usuários ou detectaram uma tentativa de instalação no período de janeiro a agosto de 2019, um aumento de 373% em relação ao mesmo período de 2018.

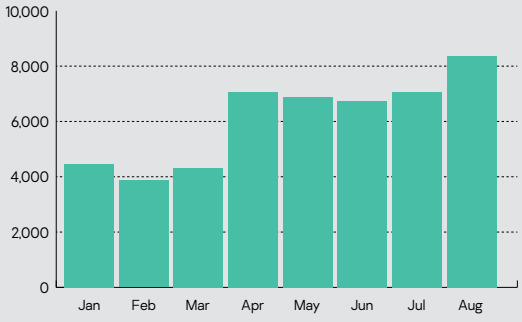


Fig.1 Número de usuários que encontraram

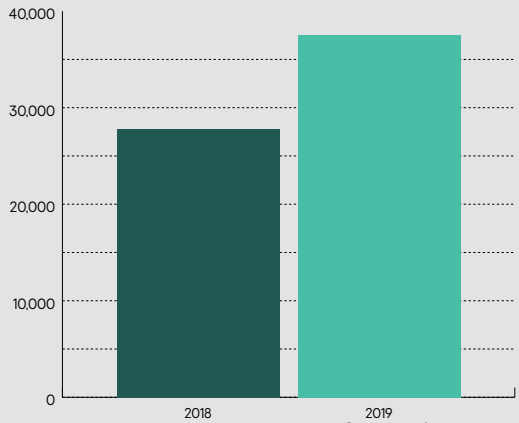


Fig.2 Usuários que foram alvos de stalkerware

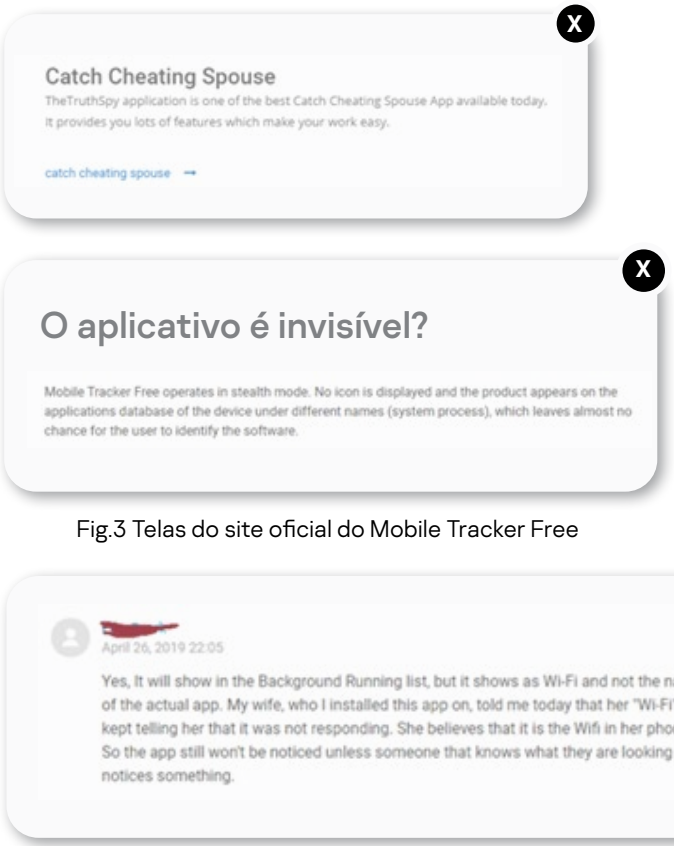


Fig.3 Telas do site oficial do Mobile Tracker Free

Fig.4 Tela do site oficial do TheTruthSpy

Exemplos de softwares usados para stalking

Terceiros também podem acessar fotos, câmera em tempo real, histórico de navegação, arquivos no dispositivo, calendário e lista de contatos nos telefones das vítimas

A família de stalkerware mais prolífica em 2019 foi identificada como Monitor.AndroidOS. MobileTracker.a, que afetou 6.559 usuários únicos. Em segundo lugar, o Monitor.AndroidOS.Cerberus.a foi detectado em dispositivos de 4.370 usuários, seguido de perto pelo terceiro lugar, o Monitor.AndroidOS.Nidb.a (4.047).

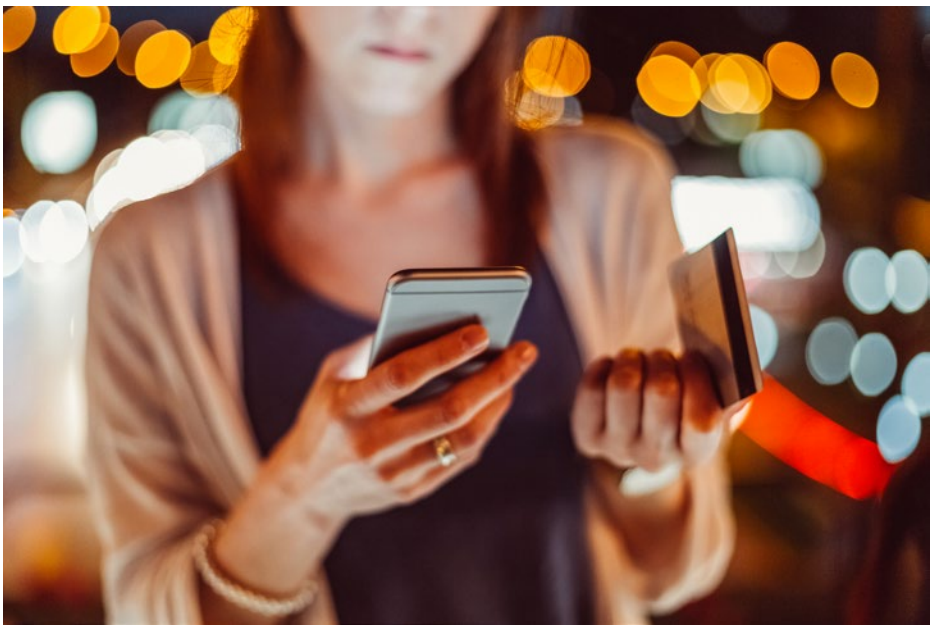
Comparando os resultados de 2018, os dois primeiros diferem do último. Monitor.AndroidOS. Nidb.a e Monitor.AndroidOS.PhoneSpy.b foram mais encontrados em 2018, atingindo 4.427 e 2.819 dispositivos de usuários, respectivamente. Monitor.AndroidOS.XoloSale.a foi o terceiro stalkerware mais comum atingindo 1.946 usuários.

Em nosso sistema interno de classificação, um registro do Monitor.AndroidOS.MobileTracker.a é usado para identificar um aplicativo Mobile Tracker Free, posicionado como uma ferramenta para rastrear a atividade de crianças ou funcionários. Na verdade, o aplicativo permite rastrear a localização do usuário, sua correspondência em mensagens SMS e outros aplicativos de mensagens (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, etc.), bem como chamadas. Terceiros também podem acessar fotos, câmera em tempo real, histórico de navegação, arquivos no dispositivo, calendário e listas de contatos das vítimas. Além disso, o aplicativo permite controlar remotamente o dispositivo. Também é possível trabalhar de modo oculto sob o disfarce de aplicativos do sistema

O próximo aplicativo, Cerberus (Monitor.AndroidOS.Cerberus.a), é classificado como um aplicativo antirroubo. No entanto, ele também permite que um stalker trabalhe em modo "oculto" e evite sua exclusão. Entre outras coisas, ele possibilita rastrear a localização do dispositivo, obter imagens da câmera e telas, além de gravar áudio do microfone.

O terceiro colocado, Monitor.AndroidOS.Nidb.a, é, na verdade, um grupo de aplicativos semelhantes: iSpyoo/TheTruthSpy/Copy9. Diferentemente dos dois aplicativos anteriores, alguns representantes desse grupo anunciam-se abertamente como um meio de espionar um parceiro e até mesmo escrever artigos sobre ele.

O conjunto de funções é bastante padrão para esses programas, mas ainda assim impressionante: rastreamento de sites, interceptação de correspondências em SMS e aplicativos mensageiros, rastreamento de chamadas e histórico de navegação. Como vários outros aplicativos semelhantes, eles exigem direitos de superusuário (direitos de administrador) para utilizar algumas funções. Eles podem operar em modo "oculto", e seus nomes na lista de aplicativos instalados imitam processos do sistema.



Onde stalkerware pode ser encontrado?

Há um mercado global para software spyware e stalkerware dentro da lei, como demonstrado pela vasta gama de regiões onde a maioria dos ataques ocorre. Os 10 principais países com mais usuários atacados por stalkerware não possuem similaridades geopolíticas e não estão próximos.

1. Federação Russa – **25,61%**
2. Índia – **10,56%**
3. Brasil – **10,39%**
4. Estados Unidos – **7,11%**
5. Alemanha – **3,55%**
6. Itália – **2,65%**
7. México – **2,10%**
8. Reino Unido – **1,95%**
9. França – **1,76%**
10. Irã – **1,68%**

Outros – **32,65%**

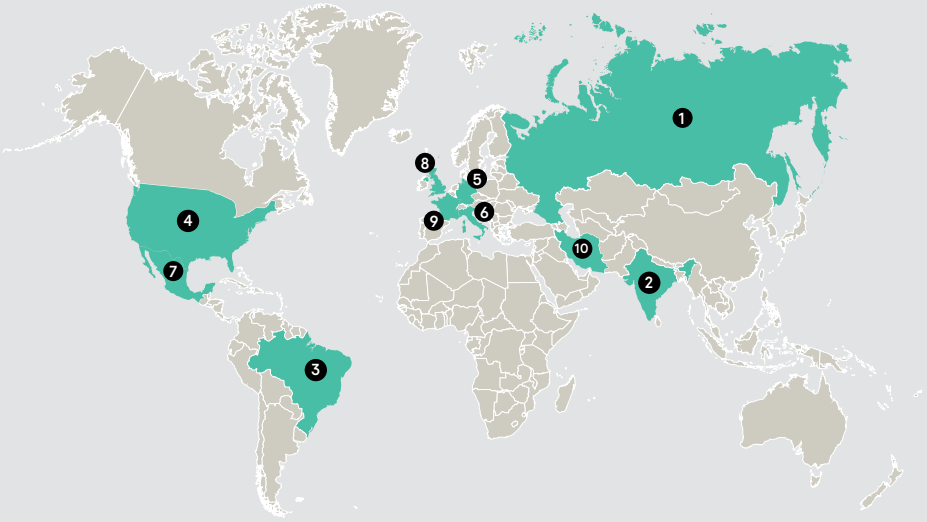


Fig. 5 Localização geográfica dos usuários afetados por

Uma pesquisa mostrou que 85% dos profissionais que trabalham com violência doméstica auxiliaram vítimas de criminosos que as rastrearam por GPS

As descobertas da Kaspersky mostram que a Rússia é a região onde a atividade de stalkerware é maior. Atividade persistente na Índia levou o país a ser a segunda região mais proeminente para incidentes relacionados a stalkerware de janeiro a agosto, com 10,56% de usuários afetados.

O Brasil contabilizou 10,39% dos usuários atacados em 2019, enquanto que os Estados Unidos são agora o quarto (7,11%). Grupos de defesa no país conscientizam as pessoas sobre os perigos de stalkerware e realizam pesquisas de usuários reveladoras. 72 abrigos de violência doméstica foram pesquisados pela National Public Radio: 85% dos profissionais que trabalham com violência doméstica declararam ter auxiliado vítimas de criminosos que as rastrearam por GPS. Quase 3/4 (71%) dos criminosos domésticos monitoram atividades nos computadores dos sobreviventes, enquanto 54% rastrearam celulares dos sobreviventes com stalkerware. O quinto país com mais evidências em 2019 foi a Alemanha (3,55%).

Stalkerware no cenário de ameaças cibernéticas

Ao comparar stalkerware e spyware com o resto dos ataques enfrentados pelos usuários de celulares, como adware, riskware e malware, eles representam uma grande proporção dos programas não vírus menos visados. Nos primeiros oito meses de 2019, a Kaspersky detectou 2.350.862 usuários atacados por possíveis ameaças indesejadas e apenas 1,60% delas foram relacionadas a stalkerware. No entanto, diferentemente da maioria das possíveis ameaças em massa (como adware), o stalkerware requer um stalker específico para agir e operar. Cada alvo é perseguido e escolhido com um propósito. Portanto, embora os números sejam mais baixos, o stalkerware promove um esforço mais direcionado à vítima e está relacionado a uma história de abuso perturbadora por trás de cada uma delas.

Para obter um panorama geral ao avaliar a dinâmica de desenvolvimento do stalkerware, comparamos stalkerware com malware de vigilância ilegal, em escala total, para PCs que detectamos como Trojan Spy. Os resultados demonstraram que spyware ilegal está em declínio e stalkerware está prosperando.

Nossa análise dos primeiros oito meses de 2019 mostra que o número de usuários que encontraram stalkerware, na verdade, suplantou o número de ataques de Trojan Spy. Enquanto em 2018 houve mais de 43.000 alvos de Trojan Spy e cerca de 28.000 alvos de stalkerware, o cenário mudou em 2019. O número de usuários que encontraram stalkerware cresceu 35% e superou 37.000, enquanto as ferramentas de spyware contabilizaram 26.620 alvos.

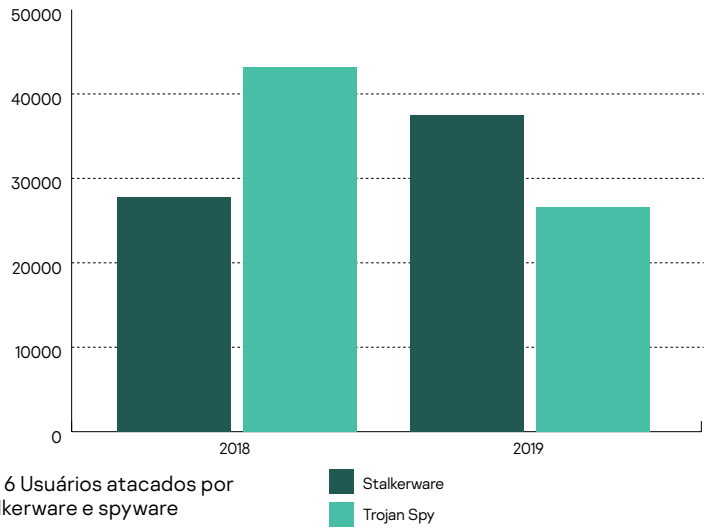
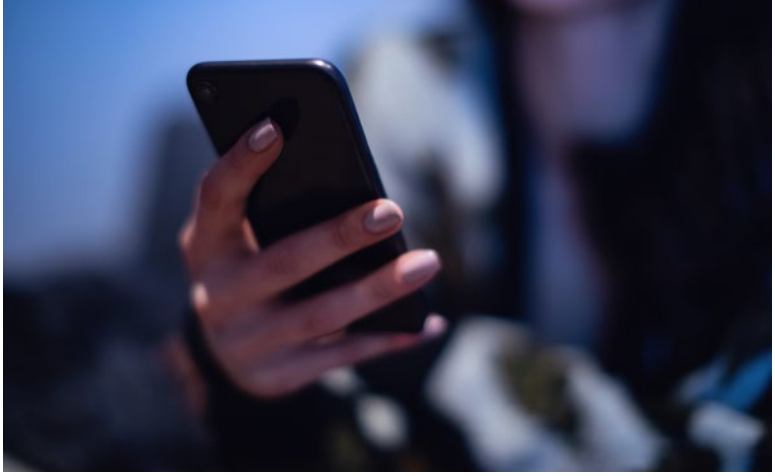


Fig. 6 Usuários atacados por stalkerware e spyware

Houve um aumento significativo do número de incidentes relacionados a stalkerware registrados por produtos Kaspersky quando comparado a todas as ameaças identificadas nos dados de 2018. Entre janeiro e agosto do último ano, esse tipo de software contabilizou apenas 1,01% do total de usuários que enfrentaram qualquer tipo de software potencialmente perigoso (adware e outros de categorias que não são vírus) (2.740.023). Parece que a popularidade do stalkerware está crescendo, enquanto os ataques de malware mais tradicionais estão sendo menos prolíficos do que há 12 meses.



Conclusão e recomendações

Está claro que stalkerware está em ascensão e se tornando muito mais proeminente no cenário da segurança cibernética. De acordo com o número geral de flutuações de ataques de riskware, adware e spyware detectados ano a ano, o percentual de incidentes relacionados a stalkerware continua crescendo. Talvez leve tempo para descobrir a função dos stalkers no cenário de ameaças cibernéticas, mas um número maior de incidentes é agora contabilizado. Graças ao aprimoramento do software de segurança cibernética, as taxas de detecção têm aumentado significativamente, desde que a Kaspersky lançou a sua própria solução para notificar usuários sobre stalkerware em abril de 2019.
Também tem sido observada uma consistência dos países mais propensos a enfrentar incidentes relacionados a stalkerware, com Rússia, Índia, Estados Unidos e Alemanha entre os mais proeminentes nos últimos dois anos.
A boa notícia para os usuários é que recursos e soluções eficazes estão sendo implementados para que eles possam se proteger. Maneiras práticas de solucionar o problema estão surgindo. Empresas de segurança de TI e organizações de advocacia que trabalham com vítimas de abuso doméstico devem juntar forças para garantir que empresas de segurança cibernética respondam melhor a stalkerware. Essas iniciativas ajudariam as vítimas por meio de tecnologia e experiência.

Acreditamos que cada pessoa tem o direito de proteger a sua privacidade. Esse é o motivo pelo qual oferecemos experiência em segurança, trabalhamos com organizações internacionais e agências policiais para combater criminosos cibernéticos e desenvolvemos tecnologias, soluções e serviços para ajudar você a se proteger contra ameaças cibernéticas.

Sobre a Kaspersky

Com mais de 20 anos de experiência em segurança cibernética, a vasta inteligência em ameaças e o conhecimento em segurança da Kaspersky estão constantemente se transformando em soluções e serviços de segurança inovadores que protegem empresas, infraestrutura crítica, governos e consumidores em várias partes do mundo. Mais de 400 milhões de usuários estão protegidos por tecnologias da Kaspersky, e ajudamos 270.000 clientes corporativos a proteger o que mais importa para eles. A cultura corporativa da Kaspersky é baseada em transparência, confiança e globalização com mais de 3.900 especialistas em 35 escritórios em 31 países.

www.kaspersky.com

www.securelist.com

kaspersky