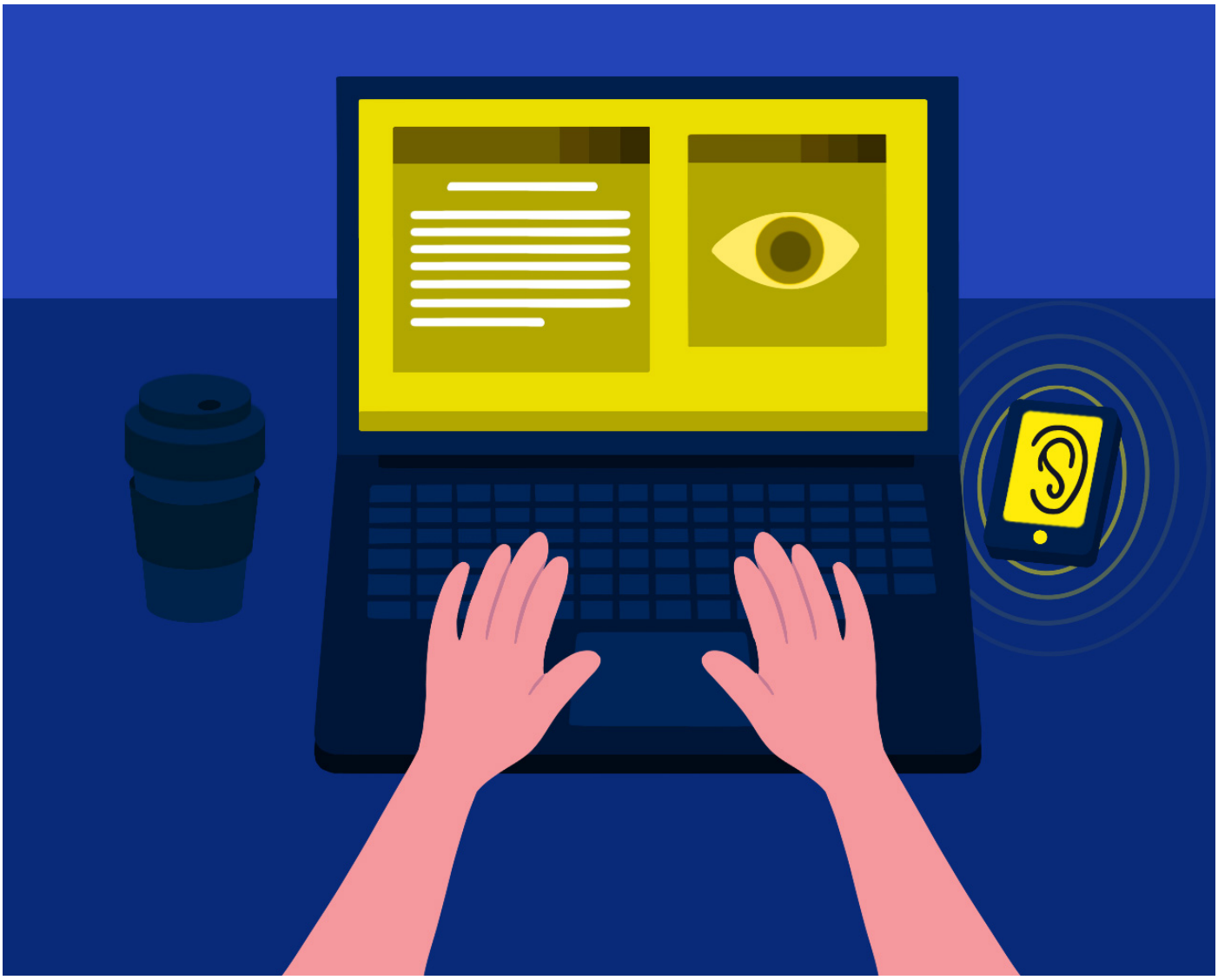


О состоянии сталкерского ПО в 2021 году

COALITION AGAINST STALKERWARE

kaspersky

Содержание

Основные данные за 2021 год

Каждый год «Лаборатория Касперского» анализирует использование сталкерского ПО во всем мире, чтобы лучше понять угрозы, которые оно представляет и эффективно с ним бороться. Мы сотрудничаем с заинтересованными лицами в государственном и частном секторах, чтобы повысить осведомленность и найти способы решения этой важной проблемы.

С помощью сталкерского ПО люди тайно следят за частной жизнью других, такие программы часто используется в целях психологического и физического насилия в отношениях. Это коммерческие программы. С их помощью можно получить доступ к большому объему персональных данных, включая местоположение устройства, историю браузера, текстовые сообщения, чаты в социальных сетях, фотографии и многое другое. Продвижение программ преследователей не запрещено законом, но использовать их без согласия человека, за которым осуществляется слежка, нельзя. Отсутствие четких законодательных ограничений во многих странах способствует распространению этих программ. Использование сталкерского ПО представляет серьезную угрозу: это нарушение конфиденциальности и форма злоупотребления техническими средствами. Требуются комплексные меры поддержки жертв и пострадавших. Для этого необходимы инновационные инструменты в законодательной, социальной и технологической сферах.

Основная статистика за 2021 год

- **По данным «Лаборатории Касперского», в 2021 году со сталкерским ПО столкнулись 32 694 уникальных пользователя во всем мире.** Эти цифры ниже, чем в 2020 году, и значительно ниже, чем в 2018 году, когда мы впервые начали собирать сведения о таких программах. Казалось бы, статистика должна внушать оптимизм, но, к сожалению, поводов для радости мало.
- **Уровень кибернасилия растет,** особенно с начала пандемии. Люди стали меньше общаться и проводить больше времени дома. В результате у абьюзеров укрепилось ощущение, что они могут контролировать своего партнера. Возможно, поэтому сталкерское ПО потеряло для них актуальность. Кроме того, к сожалению, в распоряжении абьюзеров есть много других технических средств для сталкинга и шпионажа. Такими же выводами с нами делятся и представители некоммерческих организаций, с которыми «Лаборатория Касперского» тесно сотрудничает и которые работают с нарушителями и жертвами сталкинга. Необходимо помнить, что упомянутая статистика включает только пользователей продуктов «Лаборатории Касперского». Она не учитывает тех, кто применяет антивирусные решения наших конкурентов по обеспечению ИТ-безопасности, а также тех, у кого на мобильных устройствах не установлены подобные продукты. Соответственно, мы видим только некоторую часть: точное число пострадавших пользователей оценить сложно, однако, по оценке членов

Коалиции по борьбе со stalkerware (Coalition against Stalkerware), эти цифры могут быть как минимум в 30 раз выше, а количество жертв во всем мире каждый год приближается к миллиону.

- По данным сети Kaspersky Security Network, **по-прежнему чаще всего сталкерское ПО используется в России, Бразилии и США.** Статистика за последние два года это подтверждает. На региональном уровне наибольшее количество пострадавших пользователей мы видим в следующих странах:
  - Германия, Италия и Великобритания (Европа);
  - Турция, Египет и Саудовская Аравия (Ближний Восток и Африка);
  - Индия, Индонезия и Вьетнам (Азиатско-Тихоокеанский регион);
  - Бразилия, Мексика и Колумбия (Латинская Америка);
  - США (Северная Америка);
  - Российская Федерация, Украина и Казахстан (Восточная Европа (кроме стран Европейского союза), Россия и Центральная Азия).
- **Наиболее часто использовались приложения сталкерского ПО** Cerberus (5575 пострадавших пользователей) и Reptilicus (4417 пострадавших пользователей). Указанные цифры включают жертв сталкинга во всем мире.

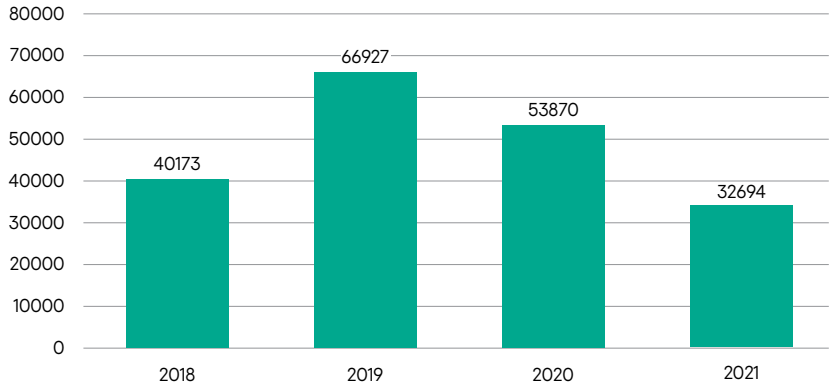
Тенденции, наблюдаемые «Лабораторией Касперского»

Показатели обнаружения во всем мире: пострадавшие пользователи

В этом разделе мы представили статистику, собранную "Лабороторией Касперского" в 2021 году во всем мире и на региональном уровне, и сравнили эти данные со сведениями предыдущих лет.

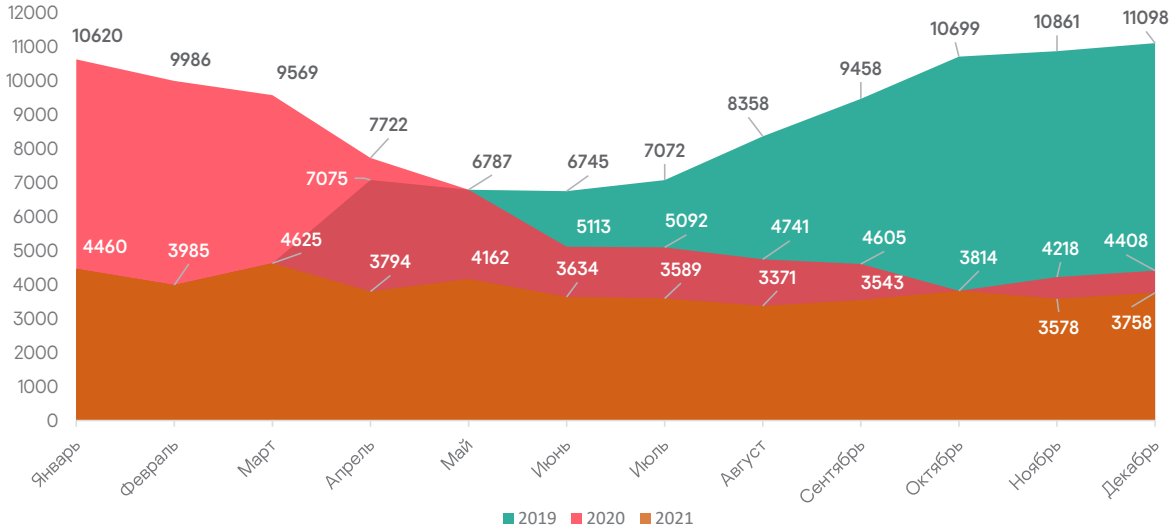
В 2021 году со сталкерским ПО столкнулись в общей сложности 32 694 отдельных пользователей

В 2021 году со сталкерским ПО столкнулись в общей сложности 32 694 уникальных пользователей. На графике ниже показано, как это количество менялось из года в год начиная с 2018 г.



Динамика числа пострадавших пользователей в годовом исчислении с 2018 года

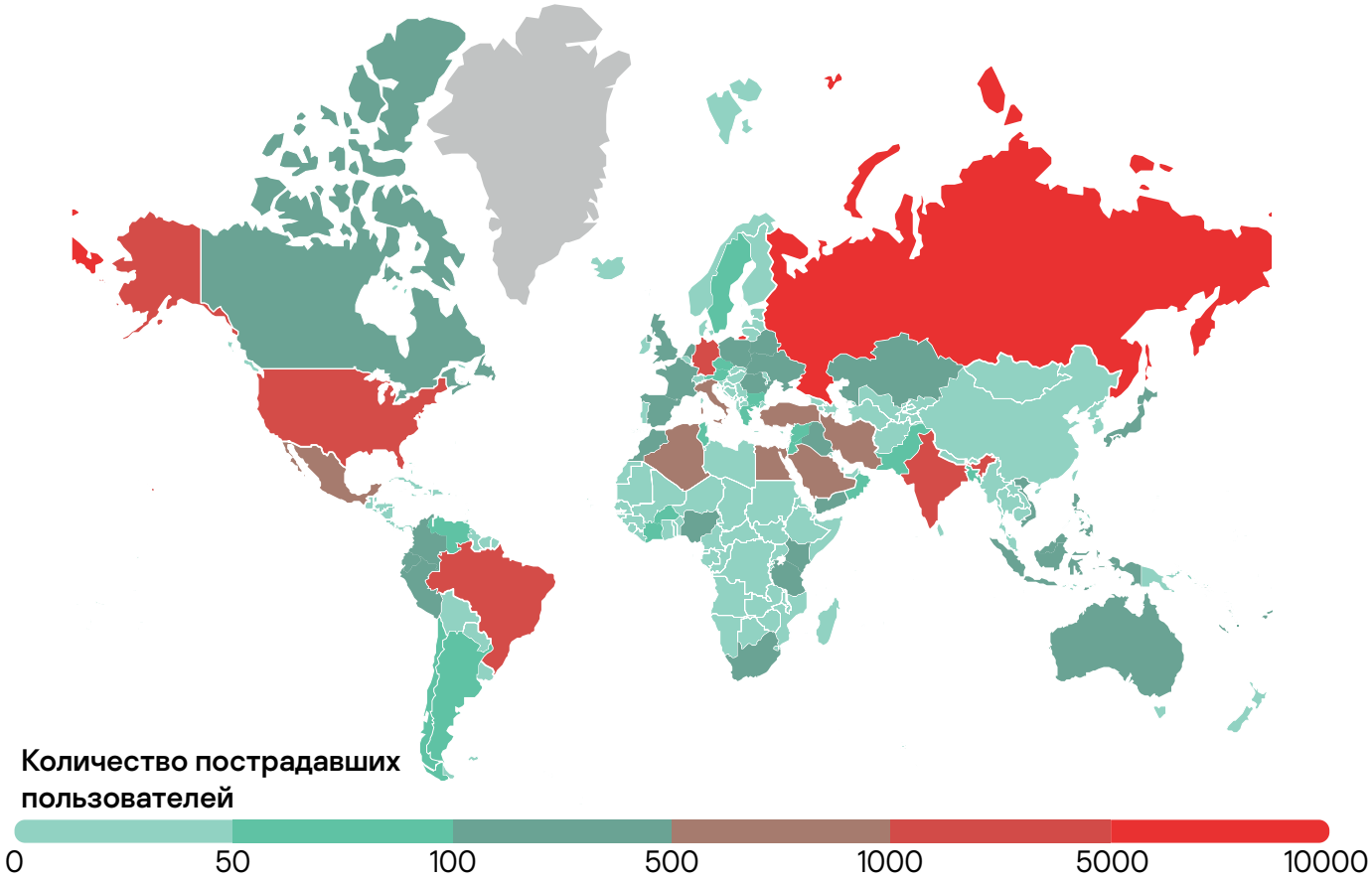
На графике ниже показано количество уникальных пострадавших пользователей в месяц в период с 2019 по 2021 год. В 2021 году ситуация более устойчивая, чем в 2020 году: в месяцы локдауна и карантинных мер количество пострадавших пользователей заметно сократилось.



Количество уникальных пользователей, затронутых в месяц в период 2019-2021 гг.

Показатели обнаружения во всем мире и в регионах: география пострадавших пользователей

Сталкерское ПО по-прежнему применяется во всем мире: в 2021 году «Лаборатория Касперского» выявила пострадавших пользователей в 185 странах или регионах.



Методология

Данные в этом отчете взяты из совокупной статистики угроз, полученной из сети Kaspersky Security Network. Kaspersky Security Network (KSN) — сложная распределенная инфраструктура, предназначенная для интеллектуальной обработки потоков данных, связанных с киберугрозами и предоставляемых добровольно миллионами пользователей по всему миру. Все полученные сведения анонимны. При расчете статистики мы учитываем только пользовательскую линейку решений «Лаборатории Касперского» для обеспечения безопасности мобильных устройств, к которой применимы критерии обнаружения сталкерского ПО, разработанные Коалицией по борьбе со сталкерским ПО. Это означает, что число пострадавших пользователей включает только тех, против кого было направлено именно сталкерское ПО. Другие типы мониторингового или шпионского ПО, которые не подпадают под определение Коалиции, не учитываются в нашей статистике.

Данные отражают число уникальных пострадавших пользователей мобильных устройств. Оно отличается от количества обнаруженных случаев использования сталкерского ПО. Число обнаруженных случаев может быть выше, так как иногда мы выявляем программы-сталкеры на одном и том же устройстве одного и того же уникального пользователя несколько раз. Такое бывает, когда пользователь получил наше уведомление, но решил не удалять приложение.

Наконец, статистика отражает только пользователей мобильных устройств, применяющих решения «Лаборатории Касперского» для обеспечения ИТ-безопасности. Некоторые могут установить на своих устройствах другое антивирусное решение, а некоторые вообще не используют подобные продукты.

Как и в 2020 году, больше всего уникальных пострадавших пользователей обнаружено в России, Бразилии, США и Индии. Интересно, что Мексика переместилась с 5-го на 9-е место, а Алжир, Турция и Египет вошли в первую десятку стран, которых использование сталкерского ПО коснулось в большей степени. Свои места им уступили Италия, Великобритания и Саудовская Аравия.

	Страна	Пострадавшие пользователи
1	Российская Федерация	7541
2	Бразилия	4807
3	США	2319
4	Индия	2105
5	Германия	1012
6	Исламская Республика Иран	891
7	Алжир	665
8	Турция	660
9	Мексика	657
10	Египет	640

Таблица 1: 10 стран мира, в которых в 2021 году было больше всего пользователей, пострадавших от сталкерского ПО

В отчете за этот год мы представили более подробную статистику по следующим регионам: Европа, Азиатско-Тихоокеанский регион, Латинская Америка, Северная Америка, Восточная Европа (кроме стран Европейского союза), Россия и Центральная Азия, а также Ближний Восток и Африка.

В Европе общее количество уникальных пострадавших пользователей в 2021 году составило 4236 человек. Германия, Италия и Великобритания, как и в предыдущем году, находятся в верхней части списка. Австрию в десятке первых стран заменила Чехия.

	Страна	Пострадавшие пользователи
1	Германия	1012
2	Италия	611
3	Соединенное Королевство Великобритании и Северной Ирландии	430
4	Франция	410
5	Польша	321
6	Испания	321
7	Нидерланды	165
8	Румыния	125
9	Бельгия	94
10	Чехия	82

Таблица 2: 10 стран Европы, в которых в 2021 году было больше всего пользователей, столкнувшихся со сталкерским ПО

В Восточной Европе (кроме стран Европейского союза), России и Центральной Азии общее количество отдельных пострадавших пользователей в 2021 году составило 9207 человек. В тройку первых стран вошли Россия, Украина и Казахстан.

	Страна	Пострадавшие пользователи
1	Российская Федерация	7541
2	Украина	490
3	Казахстан	461
4	Белоруссия	250
5	Узбекистан	223
6	Азербайджан	92
7	Республика Молдова	51
8	Таджикистан	49
9	Киргизия	40
10	Туркменистан	19

Таблица 3: 10 стран Восточной Европы (кроме стран Европейского союза), Центральной Азии, а также России, в которых в 2021 году было больше всего пользователей, столкнувшихся со сталкерским ПО

В регионе Ближнего Востока и Африки общее количество пострадавших пользователей составило 6270 человек. Больше всего их в Турции, Египте и Саудовской Аравии.

	Страна	Пострадавшие пользователи
1	Турция	660
2	Египет	640
3	Саудовская Аравия	575
4	Кения	271
5	Южная Африка	240
6	Объединенные Арабские Эмираты	143
7	Нигерия	123
8	Кувейт	68
9	Оман	58
10	Эфиопия	46

Таблица 4: 10 стран, пострадавших от сталкерского ПО в 2021 году - Ближний Восток и Африка

В Азиатско-Тихоокеанском регионе общее количество пострадавших пользователей составило 4243 человека. Индия значительно опередила другие страны: на нее приходится 2105 пострадавших пользователей. На втором месте — Индонезия, а на третьем — Вьетнам.

	Страна	Пострадавшие пользователи
1	Индия	2105
2	Индонезия	353
3	Вьетнам	258
4	Филиппины	240
5	Малайзия	229
6	Австралия	205
7	Бангладеш	169
8	Япония	167
9	Пакистан	98
10	Шри-Ланка	83

Таблица 5: 10 стран Азиатско-Тихоокеанского региона, где в 2021 году было больше всего пользователей, столкнувшихся со сталкерским ПО

Среди стран Латинской Америки и Карибского бассейна доминирует Бразилия. В ней проживает 72,5 % от общего количества пострадавших пользователей в регионе. При этом ее население составляет приблизительно 32 % от населения региона. За Бразилией следуют Мексика и Колумбия. Всего в регионе было обнаружено 6609 пострадавших пользователей.

	Страна	Пострадавшие пользователи
1	Бразилия	4807
2	Мексика	657
3	Колумбия	202
4	Эквадор	192
5	Перу	179
6	Аргентина	90
7	Чили	73
8	Венесуэла	58
9	Боливия	46
10	Гаити	36

Таблица 6: 10 стран Латинской Америки, где в 2021 году было больше всего пользователей, столкнувшихся со сталкерским ПО

Наконец, в Северной Америке 87 % всех пострадавших пользователей в регионе приходится на США. Это ожидаемые цифры, так как в этой стране проживает в десять раз больше людей, чем в Канаде. Общее количество пострадавших пользователей в Северной Америке, за исключением Мексики, которая учтена в статистике по Латинской Америке, составляет 2666 человек.

	Страна	Пострадавшие пользователи
1	США	2319
2	Канада	347

Таблица 7: количество пользователей, столкнувшихся со сталкерским ПО в 2021 году – Северная Америка

Общие функции сталкерского ПО

В этом разделе перечислены приложения сталкерского ПО, которые наиболее часто используются для контроля мобильных устройств во всем мире. Самыми популярными из них в 2021 году были Cerberus (5575 пострадавших пользователей) и Reptilicus (4417 пострадавших пользователей).

	Название приложения	Пострадавшие пользователи
1	Cerberus	5,575
2	Reptilicus (другое название 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

Таблица 8: список самых популярных приложений сталкерского ПО в 2021 году

Приложения сталкерского ПО — это способ получить контроль над жертвой и доступ к данным другого человека. Их возможности различаются в зависимости от вида приложения и от того, платное оно или бесплатное. Некоторые из них преподносятся как приложения для защиты от кражи или для родительского контроля, однако на самом деле кардинально отличаются от них. Взять хотя бы тот факт, что сталкерское ПО работает в скрытом режиме, без согласия и уведомления человека, за которым осуществляется слежка.

Вот общие функции, которые могут быть в приложениях сталкерского ПО:

- скрытие значка приложения;
- чтение SMS, MMS и журналов вызовов;
- получение списка контактов;

Угрожает ли сталкерское ПО пользователям Android и iOS в равной степени?

На устройствах iOS приложения сталкерского ПО встречаются реже, чем на устройствах Android, так как iOS традиционно является более закрытой системой. Злоумышленники могут обойти ограничение на устройствах iPhone, осуществив "джейлбрейк". Однако для этого потребуется физический доступ к телефону. Пользователям iPhone, которые опасаются, что за ними может быть установлена слежка, рекомендуется всегда держать телефон при себе.

Кроме того, абьюзер может предложить своей жертве iPhone или любое другое устройство с предустановленным сталкерским ПО. Есть множество компаний, которые предоставляют такие услуги в Интернете. Таким образом абьюзер может установить инструменты слежения на новый телефон и затем отправить его жертве в качестве подарка в заводской упаковке.

- отслеживание местоположения с помощью GPS;
- доступ к календарю;
- чтение сообщений из популярных мессенджеров и социальных сетей, таких как 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 и т. д.;
- просмотр фотографий и изображений из фотогалереи смартфона;
- создание скриншотов;
- съемка фотографий с фронтальной камеры (режим селфи).

Использование сталкерского ПО снижается, но насилие не уменьшается

Количество пострадавших пользователей, а также отношение людей к использованию сталкерского ПО по-прежнему вызывают обеспокоенность

Несмотря на то, что число пострадавших пользователей снизилось на 39% по сравнению с 2020 годом, борьба со сталкерским ПО и кибернасилием ещё далека от завершения. Количество пострадавших пользователей, а также отношение людей к использованию сталкерского ПО по-прежнему вызывают обеспокоенность. В ноябре 2021 года «Лаборатория Касперского» провела глобальный опрос с участием более 21 000 человек в 21 стране, чтобы выяснить их отношение к нарушению конфиденциальности и цифровому сталкингу в близких отношениях. Большинство респондентов (70 %) высказались, что считают неприемлемой слежку за своим партнером. Однако значительная часть опрошенных (30 %), как оказалось, не видит в этом никакой проблемы и допускает слежку в определенных обстоятельствах. Из тех, кто считает, что скрытое наблюдение может быть оправданным, почти две трети респондентов применили бы его в случае подозрения неверности партнера (64%) или в целях собственной безопасности (63%), а половина опрошенных — если бы подозревали партнера в преступной деятельности (50%).

Информационно-коммуникационные технологии (ИКТ) — это мощные инструменты для тех, кто осуществляет насильственный контроль. Особенно это касается отношений, в которых насилие присутствует и в реальной жизни

Высокоскоростной Интернет в сочетании со стремительным распространением информационно-коммуникационных технологий (ИКТ) способствует киберанасилию. Для абьюзеров это ещё один инструмент, который позволяет делиться опасными материалами или совершать действия, способные нанести эмоциональный, психологический или физический вред. Информационные технологии позволяют людям поддерживать социальные и эмоциональные связи даже на значительном расстоянии, но в то же время ими могут пользоваться для кибернасилия, а его негативные последствия распространяются уже и на реальную жизнь жертв.

Результаты нашего опроса подтверждают это: 15% респондентов по всему миру подтвердили, что сталкивались с требованием партнера установить приложение для мониторинга, а 34% из них — подвергались физическому и/или вербальному насилию со стороны того же человека.

Хотя делать категоричные выводы насчет снижения числа пострадавших пользователей в 2021 году ещё слишком рано, есть две теории, которые могли бы объяснить эту тенденцию.

Во-первых, мы считаем, что пандемия по-прежнему оказывает сильное влияние на все аспекты нашей жизни. Недавние исследования показали, что в различных сферах жизни, таких как работа, учеба, дом, потребление, коммуникации и информация, путешествия и мобильность, возникают новые модели поведения. Если коротко, то речь вот о чем: люди стали проводить больше времени дома (49 % опрошенных стараются реже выходить из дома, а 50 % работают из дома частично или полностью), меньше путешествовать и общаться вживую (57 % респондентов заявили о том, что они дистанцируются от друзей и знакомых), а также все чаще совершать покупки, учиться и находить развлечения в Интернете. Возможно, сталкерское ПО не так востребовано у абьюзеров, ведь партнер и так большую часть времени на виду.

Во-вторых, Интернет вещей (IoT) и цифровизация уже прочно вошли в нашу жизнь. Мы используем их в наших повседневных делах, в доме, в машине, в офисе. С одной стороны, благодаря этому у нас появилась масса новых возможностей, с другой — такие устройства не всегда используются людьми в благих целях. Как показало наше исследование, абьюзеры могут следить за своими партнерами и с помощью других средств, помимо сталкерского ПО. Вот что говорят участники опроса: 50% из них подверглись слежке через приложение для телефона, 29% — через устройства отслеживания, 22% — через веб-камеры и 18% — через устройства для умного дома.

Публикация в январе 2022 года руководства по технике безопасности для устройств AirTag компании Apple свидетельствует об изменении отношения к таким ситуациям.

Национальная сеть по прекращению домашнего насилия (NNEDV) и Европейская сеть по работе с субъектами домашнего насилия (WWP EN) поделились с нами своим опытом, а также взглядами на упомянутые выше две теории и мнением о злоупотреблении техническими возможностями в целом.

О том, как меры, принятые правительствами во время пандемии, способствовали усилению насильственного контроля, нам рассказали Берта Валль Кастелло, менеджер по исследованиям и развитию, и Анна Маккензи, менеджер по коммуникациям в WWP EN

Под насильственным контролем понимается «модель абьюзивного поведения, цель которого — проявление доминирования и власти над другим человеком». При этом абьюз может проявляться в разных формах — физической, психологической, эмоциональной или финансовой. В результате всего этого жертва через какое-то время перестает быть автономной и независимой личностью» (Макгоррери и Макмахон, 2020 г.). Партнеры, совершающие насилие, изолируют свою жертву и вовлекают ее в эмоциональную зависимость. Об этом мы писали в нашем руководстве «То же самое насилие, но с помощью новых средств: как работать с мужчинами, которые применяют кибернасилие» (Same Violence, New Tools – How to work with violent men who use cyberviolence). С помощью оскорблений, угроз, запугивания, унижения, изоляции и других методов такие люди вызывают у жертвы постоянное чувство страха и отсутствия свободы. Информационно-коммуникационные технологии (ИКТ) — это мощные инструменты для тех, кто осуществляет насильственный контроль. Особенно это касается отношений, в которых насилие присутствует и в реальной жизни.

Недавнее исследование о домашнем насилии в период пандемии COVID-19 показало, что меры, принятые правительствами в тот период, способствовали усилению насильственного контроля. Как предполагают авторы исследования, условия изоляции и физического дистанцирования соответствовали стратегиям тех, кто осуществляет насильственный контроль над партнерами (Пентараки и Спик, 2020 год). На основании этого можно сделать вывод, что в новых условиях для насильственного контроля за партнерами уже нет большой необходимости в использовании сталкерского ПО. Более того, согласно недавнему исследованию, абьюз с использованием технологических средств наблюдается гораздо чаще в период, когда партнеры живут отдельно друг от друга (Джордж и Харрис, 2014 г., Вудлок, 2016 г.). Таким образом, в ситуации локдауна, когда пары вынуждены оставаться вместе дома, вероятность такого вида насилия снижается.

WWP EN

Европейская сеть по работе с субъектами домашнего насилия (WWP EN) является членской ассоциацией организаций, которые напрямую или опосредованно работают с людьми, совершающими насилие в отношении близких людей. Основное внимание в WWP EN уделяется насилию мужчин в отношении женщин и детей. Целью WWP EN является повышение безопасности женщин, детей, а также других лиц, подверженных риску насилия со стороны близких людей, посредством продвижения эффективной работы с теми, кто совершает насилие, — в основном это мужчины.

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

При этом мы должны помнить: тот факт, что сталкерское ПО стало использоваться реже, не означает снижение уровня общего насилия со стороны партнеров во время пандемии COVID-19. Как раз наоборот: Боксалл, Морган и Браун (2020 г.) отмечают его рост в этот период. Таким образом, результаты этого отчета показывают, что вместо сталкерского ПО стали использоваться другие инструменты. Елена Гаджотто из итальянской неправительственной организации Una Casa per l'Uomo, отмечает: «Следить за кем-либо, например, с помощью учетной записи Google этого человека, совсем не сложно. Так что особой необходимости в сталкерском ПО нет». Вполне возможно, что широкий спектр способов абьюза с помощью технологических средств привел к сокращению случаев использования сталкерского ПО. Так же считает Летиция Барончелли, из итальянской неправительственной организации Centro Ascolto Uomini Malttratanti (CAM). Вот что она говорит: «Я думаю, пользоваться сталкерским ПО стали реже, так как есть много других форм цифрового абьюза».

Меры, принятые правительствами в тот период, способствовали усилению насильственного контроля

Вместе с тем неправительственные организации, органы государственной власти и независимые исследователи сообщают о значительном росте случаев абьюза в форме распространения фотографий и сексуального шантажа с начала пандемии (Бониелло, 2020 г.; Колледж Род-Айленда (CCRI), личное общение, 2 июня, 2020 г; ФБР, 2020 г., 2021 г.). Этот вид абьюза стал особенно распространенным среди подростков и партнеров, которые не живут вместе. Летиция Барончелли отмечает: «С момента начала пандемии сильно участились случаи распространения личных фотографий, особенно среди молодежи. Те, кто этим занимается, не понимают, что это преступление». Елена Гаджотто добавляет: «Абьюз посредством распространения фото наносит разрушительный вред женщинам, против которых он направлен. При этом мужчины даже не понимают, что они совершили что-то плохое».

Несколько участников сети WWP EN поделились информацией о том, что наиболее распространенной формой цифрового насилия является мониторинг цифровой деятельности партнеров, например путем проверки электронных писем, телефонов и учетных записей в социальных сетях. Это подтверждают и наблюдения Дэниэла Антуновича из хорватской неправительственной организации UZOR. Он согласен с тем, что самые примитивные формы цифрового сталкинга встречаются чаще всего.

Представители сети WWP EN считают, что для обеспечения безопасности жертвы необходимо особое внимание уделять формам абьюза, связанным с использованием технологий. Елена Гаджотто добавляет: «Около половины мужчин, которые совершают цифровое насилие, даже не догадываются, что это абьюз. Если мы не начнем акцентировать на нем внимание в нашей

работе с теми, кто совершает насилие, понимание этого так и не придет». Таким образом, есть необходимость в увеличении количества специалистов, которые работают с абьюзерами и жертвами домашнего насилия. Они смогут выявлять случаи цифрового насилия и вмешиваться в таких ситуациях. Дэниэл Антунович добавляет: «Случаев цифрового насилия, с которыми мы столкнулись, оказалось меньше, чем я ожидал с начала пандемии COVID-19. Однако абьюз с помощью технологий в некоторой степени похож на сексуальное насилие. Оно случается часто, но многие о нем умалчивают».

По словам Тоби Шалраффа, руководителя проектов по технической безопасности в NNEDV, наблюдается рост числа «умных» устройств, которые используются в целях насилия со стороны интимного партнера.

Помимо сталкерского ПО есть много других похожих инструментов для технологического насилия. Например, можно узнавать о местоположении человека или отслеживать его активность с помощью личных данных, доступных в Интернете, а также обычных функции устройств и учетных записей. Жертвам абьюзеров и людям, которые работают с ними, бывает сложно разобраться в связях между устройствами, аккаунтами и информацией в Интернете и оценить происходящее, чтобы принять эффективные меры. Страшно осознать, что в распоряжении абьюзера есть масса сведений о твоей повседневной жизни.

К сожалению, появляется все больше «умных» устройств, которые становятся средствами насилия со стороны романтического партнера: это в том числе домашние помощники, подключенные устройства и системы безопасности, подключенные к сети Wi-Fi и смартфонам.

Опрос, проведенный сетью NNEDV в декабре 2020 г. и январе 2021 г., свидетельствует о росте всех видов технологического насилия в период пандемии. Больше всего злоупотребляют использованием телефонов: согласно оценке потребностей, проведенной NNEDV, это происходит в 87% случаев. Однако все чаще в целях технологического насилия применяются «умные» или подключенные устройства — с такими случаями сталкивались около трети специалистов, оказывающих поддержку жертвам насилия.

NNEDV

Проект NNEDV «Безопасная сеть» (Safety Net) направлен сразу на несколько сфер: технологии, защита личных данных, конфиденциальность и инновации. Его цель — решение проблем безопасности и абьюза посредством разработки правил, обучения специалистов в системе правосудия, а также работы с сообществами, агентствами и технологическими компаниями. Все это поможет создать меры против злоупотребления технологиями, обеспечить поддержку жертв насилия в использовании технологий и улучшить работу сервисов.

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

Появляется все больше «умных» устройств, которые становятся средствами насилия со стороны романтического партнера: это в том числе домашние помощники, подключенные устройства и системы безопасности, подключенные к сети Wi-Fi и смартфонам

По мере того, как все больше людей используют устройства Интернета вещей, количество таких продуктов будет расти. Производство подобных устройств, предназначенных для повышения удобства и эффективности, быстрыми темпами растет во всем мире. Им занимаются как крупные, давно работающие на рынке предприятия, так и большое количество маленьких, новых компаний[1]. Интернет вещей появился благодаря нескольким взаимосвязанным технологическим тенденциям: миниатюризации, повышению обрабатывающей способности, увеличению объема хранения данных, снижению стоимости производства и появлению возможностей подключения.

Из-за различных факторов: давления рынка, быстрого появления технологии и сложности Интернета вещей – становятся все более очевидными[2] значительные риски для безопасности и конфиденциальности. В частности, для насилия со стороны романтических партнеров используются устройства умного дома. Они применяются с цель контроля, угроз и причинения вреда жертвам. [Изучением этого вреда занимаются исследователи, задействованные в проекте «Пол и Интернет вещей» (Gender + IoT) Университетского колледжа Лондона[3].] [Они сотрудничают со специалистами, оказывающими поддержку жертвам насилия, и предлагают меры, которые помогут устранить последствия этого вреда.]

Данные недавней оценки потребностей, проведенной NNEDV, свидетельствуют о появлении все большего количества способов технологического насилия во время пандемии. Мы обеспокоены тем, что, когда кризисный период закончится, абьюзеры, привыкшие к этим новым способам и ставшие ещё больше злоупотреблять технологическими возможностями, будут продолжать это делать и дальше. По мнению авторов исследования[4], специалисты, оказывающие поддержку жертвам насилия, должны спрашивать их о любых видах технологического насилия, в том числе об использовании сталкерского ПО и устройств умного дома. Существует большая вероятность того, что рост технологического насилия, который наблюдают специалисты поддержки, сохранится. Мы обязательно должны продолжать оказывать помощь жертвам и дальше работать над предотвращением технологического насилия.

---

1 Internet Society. (2015 г.). Интернет вещей: обзор. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf или https://www.internetsociety.org/iot/

2 Internet Society. (2015 г.). Интернет вещей: обзор. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf или https://www.internetsociety.org/iot/

3 Танцер Л., Нейра И. Л., Паркин С., Пейтел Т. и Данезис Дж. (2018 г.). Распространение Интернета вещей и его влияние на злоупотребление технологиями. Университетский колледж Лондона.

4 Фрид Д., Палмер Дж., Минчала Д., Леви К., Ристенпарт Т. И Делл Н. (2017 г.). Цифровые технологии и насилие со стороны интимных партнеров: качественный анализ с учетом интересов разных сторон. Разработки Ассоциации вычислительной техники ACM в отношении взаимодействия «человек-компьютер», 1(CSCW), стр.1–22.

Как «Лаборатория Касперского» и ее партнеры вместе ведут борьбу со сталкерским ПО

Угроза использования сталкерского ПО — это не только техническая проблема. В ее решение должны быть вовлечены все общественные институты. В течение последних нескольких лет «Лаборатория Касперского» активно участвует в дискуссиях на тему сталкерского ПО. Чтобы лучше разобраться в этой проблеме, мы обращаемся к заинтересованным лицам в общественной и частной сферах. Мы участвуем в разработке учебных материалов и практических инструментов для поддержки некоммерческих организаций, корпораций, учреждений и частных лиц с целью повышения устойчивости к сталкерскому ПО. Чтобы делиться своим опытом, мнением и вносить свой вклад в дискуссии, которые повлияют на будущее законодательство, мы организуем вебинары и круглые столы с представителями разных учреждений и сами принимаем участие в таких мероприятиях.

«Лаборатория Касперского» является одним из основателей и активных членов Коалиции по борьбе со stalkerware (CAS) — международной рабочей группы по борьбе со сталкерским ПО и домашним насилием. Коалиция объединяет организации, которые работают с абьюзерами и их жертвами, активистами в Интернете, а также компаниями, занимающимися вопросами кибербезопасности. Это уникальная платформа, которая позволяет всем заинтересованным сторонам обмениваться опытом и объединять усилия для решения проблемы сталкерского ПО.

«Лаборатория Касперского» также является одним из партнеров проекта DeStalk. Это исследовательский проект, финансируемый Европейской комиссией. Он направлен на то, чтобы разработать стратегию обучения и поддержки специалистов, которые работают в службах помощи жертвам насилия и программах для насильников, а также сотрудников государственных учреждений, местных органов власти и других заинтересованных групп. Консорциум планирует обновить и протестировать существующие инструменты для специалистов, а также разрабатывает региональную пилотную кампанию по повышению осведомленности в Италии.

В 2021 году мы совместно с INTERPOL и двумя уважаемыми некоммерческими организациями из США и Австралии провели два онлайн-тренинга для сотрудников правоохранительных органов. Эти курсы прошли более 210 участников со всего мира.

В конце 2021 года «Лаборатория Касперского» также приняла участие в мероприятии, организованном Советом Европы, «Борьба с насилием в отношении женщин в цифровую эпоху: применение Стамбульской конвенции». На нем обсуждались рекомендации группы экспертов по борьбе с насилием над женщинами и домашним насилием (GREVIO).

TinyCheck: инструмент для поддержки жертв домашнего насилия

Стоит отдельно коснуться такой инициативы «Лаборатории Касперского», как TinyCheck. Это бесплатный инструмент с открытым исходным кодом, разработанный и поддерживаемый «Лабораторией Касперского». Изначально TinyCheck был создан для помощи неправительственным организациям в защите жертв домашнего насилия и их конфиденциальных данных. Он позволяет легко, быстро и без вмешательства выявить использование сталкерского ПО на устройстве с любой операционной системой без ведома человека, который его установил. Обычные решения по обеспечению безопасности также могут проверить устройство на наличие сталкерского ПО и уведомить о нем, однако их необходимо устанавливать на устройство. Поэтому есть риск, что правонарушитель узнает о такой проверке. Благодаря инструментам, подобным TinyCheck, жертвы насилия пользуются своими устройствами и не переживают, что их действия могут отслеживаться.

TinyCheck позволяет легко, быстро и без вмешательства выявить использование сталкерского ПО на устройстве с любой операционной системой без ведома человека, который его установил

Чтобы проверить устройство с помощью TinyCheck, ничего устанавливать не нужно. Результаты проверки не отображаются и не передаются на само устройство. Кроме того, TinyCheck позволяет проверить устройство с любой операционной системой: iOS, Android и др. Таким образом, инструмент решает две основные проблемы, связанные с защитой пользователей от сталкерского ПО. Он работает на Raspberry Pi с обычным подключением к Wi-Fi. TinyCheck быстро анализирует исходящий трафик мобильного устройства и определяет индикаторы компрометации (IOC), такие как взаимодействия с известными вредоносными источниками, например серверами, связанными со сталкерским ПО. В настоящее время инструмент использует индикаторы компрометации, собранные не только сотрудниками «Лаборатории Касперского», но и независимыми исследователями. Особенно мы благодарны Этьену Мэнье из компании Echap, также известному как Tek, и Циану Хисли. Мы надеемся, что сообщество продолжит эту работу и будет поддерживать актуальность IOC.

И все же надо понимать, что у TinyCheck также есть ограничения. Используя его, следует иметь в виду: в отличие от решений по обеспечению ИТ-безопасности индикаторы компрометации не обеспечивают полное обнаружение в режиме реального времени всех приложений сталкерского ПО. Таким образом, не исключено, что инструмент TinyCheck может не обнаружить приложение для слежки, установленное на устройстве.

В 2021 году инструмент TinyCheck был протестирован несколькими неправительственными организациями по борьбе с домашним насилием. Отзывы о его использовании помогут улучшить сервис. К TinyCheck как инструменту для помощи жертвам насилия проявили интерес также полиция и правоохранительные органы нескольких стран.

Положительные изменения в сфере законодательства и на уровне органов власти в 2021 году

В 2021 году произошли некоторые положительные сдвиги в борьбе со сталкерским ПО на законодательном уровне и на уровне органов власти. В мае 2021 года, парламент Японии принял законопроект о внесении изменений в закон этой страны, регулирующий сталкинг. В частности, новыми нормами признается незаконным получение информации о местоположении пользователей смартфонов через приложения без их разрешения.

В августе 2021 года Федеральная торговая комиссия США запретила одному из производителей приложений предлагать сталкерское ПО. Это был первый запрет такого рода.

17 августа 2021 года германский Бундестаг принял закон о внесении изменений в Уголовный кодекс — «О более эффективных средствах борьбы со шпионскими программами и кибersталкингом» (перевод с немецкого языка). Новый закон вступил в силу 1 октября 2021 года, и теперь кибersталкинг считается в Германии преступлением. Изменение связано с тем, что из-за того, что люди все активнее пользуются возможностями продолжающегося технологического прогресса число случаев кибersталкинга растет. В частности, это касается использования шпионских приложений или сталкерского ПО. Также важно то, что новый закон классифицирует преступление как серьезное, если «в процессе его совершения используется компьютерная программа, целью которой является цифровая слежка за другими людьми».

Очень активно над этой темой работал в 2021 году Совет Европы. В своей первой рекомендации, касающейся насилия в отношении женщин в «цифровом измерении», Группа экспертов Совета Европы по борьбе с насилием в отношении женщин и домашним насилием (GREVIO) определяет и описывает проблемы гендерного насилия над женщинами, совершаемого в Интернете, и технологического насилия в отношении них, например с помощью допускаемых законом отслеживающих устройств. Вскоре после этого в декабре 2021 года был создан отчет законодательной инициативы, касающейся гендерного кибернасилия.

Он был принят Европейским парламентом. В отчете говорится о необходимости (i) дать общее определение гендерного кибернасилия и (ii) создать возможности для заинтересованных сторон. Также в нем подчеркивается, что использование сталкерского ПО является одним из способов кибернасилия, и указывается, что «приложения для скрытой слежки нельзя считать приложениями для родительского контроля». Положения этого отчета, принятого вслед за общими рекомендациями Совета Европы, не являются обязательными. Однако он представляет собой ещё один официальный документ, в котором освещается проблема сталкерского ПО и который подтолкнет государства Европы к изменению законодательства для ее решения. Наконец, 8 марта 2022 года Европейская комиссия опубликовала предложение для Директивы Европейского парламента и Совета по борьбе с насилием в отношении женщин и домашним насилием. Этот документ касается кибернасилия. Две статьи в нем посвящены киберсталкингу (ст. 8) и кибердомогательствам (ст. 9) — эти действия предлагается криминализировать.

Что делать, если вам кажется, что в отношении вас применяется сталкерское ПО? Несколько советов

Если вам нужна помощь, обратитесь в местную организацию поддержки. Чтобы найти ближайшую к вам организацию, зайдите на сайт Коалиции против сталкерского ПО.

Независимо от того, столкнулись ли вы с использованием сталкерского ПО в отношении вас или нет, эти советы помогут обеспечить вашу безопасность:

- Защитите свой телефон надежным паролем, и не сообщайте его никому, в том числе близким друзьям или коллегам.
- Периодически меняйте пароли всех своих учетных записей.
- Загружайте приложения только из официальных источников, таких как, например Google Play или Apple App Store.
- Установите на свои устройства надежное решение для обеспечения ИТ-безопасности, например Kaspersky Internet Security для Android, и регулярно сканируйте их. Однако, если есть вероятность того, что программа для слежки уже установлена, сначала следует оценить все риски. Абьюзер может заметить, что используется решение для кибербезопасности.

Жертвами сталкерского ПО могут быть люди, которые подвергаются и другим видам насилия, в том числе физическому. В некоторых случаях правонарушитель может получать уведомления о том, что жертва сканирует устройство или удаляет приложение для слежки. Это может только усугубить ситуацию и вызвать ещё большую агрессию. Вот почему важно действовать обдуманно, если вы предполагаете, что в отношении вас применяется сталкерское ПО.

- **Обратитесь в местную службу поддержки.** Ближайшую к вам подобную организацию можно найти на сайте Коалиции по борьбе со stalkerware.
- **Обращайте внимание на следующие предупреждающие знаки:** быстро разряжающийся аккумулятор (это может быть из-за неизвестных или подозрительных приложений на устройстве) и недавно установленные приложения с подозрительными функциями доступа к информации о вашем местоположении, а также отправки и получения текстовых сообщений или других личных действий. Также проверьте, включен ли у вас параметр «неизвестные источники». Это может быть признаком того, что на устройстве было установлено нежелательное стороннее программное обеспечение. Важно отметить, что указанные выше признаки являются косвенными и не указывают на однозначное наличие сталкерского ПО.
- **Не пытайтесь сразу удалить сталкерское ПО, изменить его настройки или настройки телефона:** таким образом вы можете уведомить потенциального насильника и усугубить ситуацию. Кроме того, совершая эти действия, вы рискуете удалить важные данные или доказательства, которые могут быть использованы правоохранительными органами для расследования.

Для получения дополнительной информации о нашей деятельности по борьбе со сталкерским ПО или любого другого запроса напишите нам по адресу ExtR@kaspersky.com.

Из-за масштаба угрозы, которую представляли программы для слежки, в ноябре 2019 года была основана **Коалиция по борьбе со сталкерским ПО.** Организация старается объединить опыт своих партнеров в области поддержки жертв домашнего насилия, работы с лицами, осуществляющими насилие, и защиты прав человека в цифровой среде для борьбы с преступным поведением, включающим использование сталкерского ПО. Все ее члены обязуются бороться с домашним насилием, сталкингом и харассментом путем решения проблемы сталкерского ПО и повышения осведомленности общества.

Коалиция против сталкерского ПО:
https://stopstalkerware.org/

COALITION AGAINST STALKERWARE

Новости о киберугрозах: www.securelist.ru
Новости ИТ-безопасности:
www.kaspersky.ru/blog/category/business
ИТ-безопасность для малого и среднего бизнеса:
www.kaspersky.ru/enterprise-security
ИТ-безопасность для предприятий:
www.kaspersky.ru/small-to-medium-business-security

www.kaspersky.ru

kaspersky