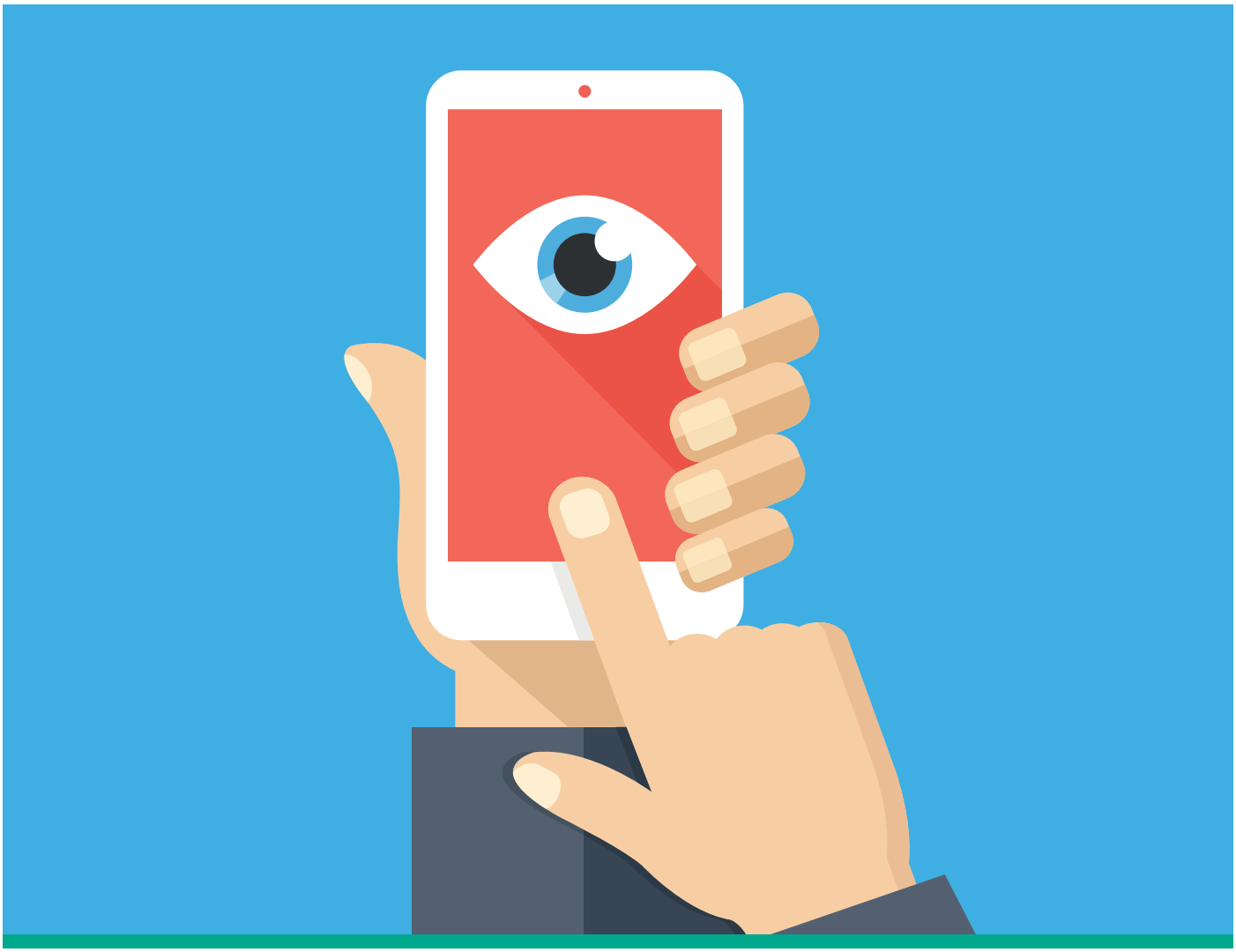


Рынок **сталкерских** программ в 2020 году

COALITION AGAINST STALKERWARE

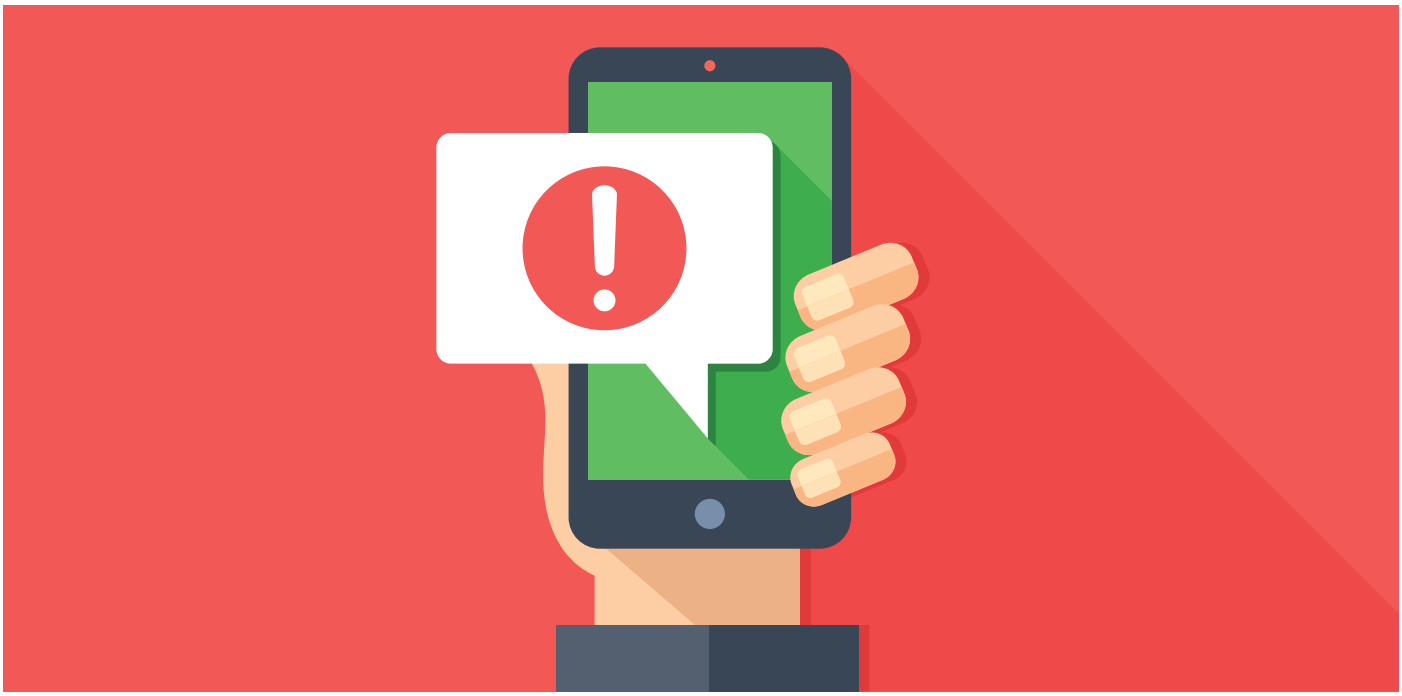
kaspersky

Содержание

Основные результаты исследования 2020 года

Данные «Лаборатории Касперского» показывают, что проблема со сталкерским ПО в 2020 году не изменилась значительно по сравнению с прошлым годом:

- Количество пользователей, столкнувшихся с этим программным обеспечением, все еще велико. В 2020 году в мире всего 53 870 мобильных пользователей пострадали от сталкерского ПО. Это цифра включает в только пользователей продуктов «Лаборатории Касперского», поэтому общее количество во всем мире будет еще выше. Некоторые пострадавшие пользователи могут использовать другое решение для обеспечения информационной безопасности на своих устройствах, а некоторые вообще их не используют.
- Nidb, от которого пострадали более 8 100 пользователей во всем мире, — является наиболее используемым образцом сталкерского ПО, согласно нашей статистике за 2020 год. Этот образец используется для продажи ряда различных продуктов сталкерского ПО, таких как iSpyoo, TheTruthSpy и Copy9, помимо других.
- Россия, Бразилия и США остаются наиболее пострадавшими странами в мире и являются тремя ведущими странами в 2020 году.
- Наиболее пострадавшие страны в Европе - Германия, Италия и Великобритания.



Введение и методология

Сегодня технологии позволяют людям оставаться на связи больше, чем когда-либо раньше. Мы делимся своей жизнью в цифровой форме с нашими семьями и друзьями независимо от того, насколько далеко мы находимся друг от друга. Однако мы также видим все большее распространение программного обеспечения, которое позволяет пользователям удаленно шпионить за жизнью другого человека, который не знает об этом и не давал на это своего согласия.

Действие сталкерского ПО может выйти за рамки онлайн-сферы и распространиться на реальную жизнь. Коалиция против сталкерского ПО предупреждает, что сталкерское ПО «может способствовать преследованию, сталкингу и/или насилию в отношении партнеров».

Программное обеспечение, известное как сталкерское ПО, или stalkerware, может скачать любой человек, имеющий доступ к Интернету. Действие сталкерского ПО может выйти за рамки онлайн-сферы и распространиться на реальную жизнь. Коалиция против сталкерского ПО предупреждает, что сталкерское ПО «может способствовать преследованию, сталкингу и/или насилию в отношении партнеров». Сталкерское ПО может также работать в скрытом режиме, когда на устройстве не отображается никакой значок, указывающий на его присутствие, и оно не видно для пользователя. Большинство пострадавших пользователей даже не знает, что такой тип программного обеспечения существует. Это означает, что они не могут защитить себя онлайн или вне сети. Более того, необходимо учитывать, что злоумышленник, использующий сталкерское ПО, обычно знает свою жертву лично.

В последние годы «Лаборатория Касперского» активно работала с партнерами над прекращением использования сталкерского ПО. В 2019 году мы создали специальное оповещение, которое уведомляет пользователей, если сталкерское ПО установлено на их телефонах. Помимо этого, мы стали одним из десяти членов-учредителей Коалиции против сталкерского ПО. Мы также опубликовали первый полный отчет о рынке сталкерского ПО в 2019, чтобы понимать масштаб проблемы.

В этом отчете продолжается исследование проблемы сталкерского ПО и представлена новая статистика за 2020 год в сравнении с нашими предыдущими данными. Данные в этом отчете были взяты из агрегированной статистики по угрозам, полученной от Kaspersky Security Network. Kaspersky Security Network предназначена для выделенной обработки потоков данных, связанных с кибербезопасностью, от миллионов добровольных участников во всем мире. Все полученные данные анонимизируются. Для расчета статистики мы рассматриваем потребительскую линейку мобильных решений по обеспечению безопасности «Лаборатории Касперского».

Проблема и история сталкерского ПО

Сталкерское ПО, или stalkerware, — это программное обеспечение, которое может приобрести любой человек, имеющий доступ в Интернет. Оно используется для удаленного шпионажа за другим человеком через его устройство. При этом пострадавший пользователь может даже не знает о нем. Сталкерское ПО работает в скрытом режиме - на устройстве не отображается никакой значок, указывающий на его присутствие, и оно не видно пользователю. Поэтому Коалиция против сталкерского ПО определяет сталкерское ПО как программное обеспечение, которое «может способствовать преследованию, сталкингуи/или насилию в отношении близких партнеров».

Размеры кибернасилия

В Европе, семь из десяти женщин, которые испытали на себе кибersталкинг, подвергались также по крайней мере одной форме физического и/или сексуального насилия от близкого партнера.

Согласно отчету Европейского института гендерного равенства «в Европе, семь из десяти женщин, которые испытали на себе кибersталкинг, подвергались также по крайней мере одной форме физического и/или сексуального насилия от близкого партнера». Подтверждая результаты исследования, эксперты из некоммерческих организаций (НКО), которые помогают пострадавшим и жертвам домашнего насилия, подчеркивают, что кибersталкинг также является формой насилия. Наряду с физическим, психологическим и экономическим насилием, злоумышленник может использовать сталкинг для получения полного контроля над жертвой/пострадавшим[1].

Использование сталкерского ПО позволяет злоумышленнику практически полностью контролировать жертву. В зависимости от установленного типа сталкерского ПО у него может быть много разных функций для вторжения в частную жизнь жертвы. С помощью программного обеспечения злоумышленник может:

- читать все, что пишет пользователь, за которым следят, — регистрируется каждое нажатие клавиши на устройстве, включая учетные данные для служб любого типа, таких как банковские приложения, интернет-магазины, социальные сети и т. д.;
- знать, где находится пользователь, путем отслеживания его перемещений с помощью GPS в режиме реального времени;
- слышать все, что говорит пользователь, — прослушивать вызовы или даже записывать их;

1 Эксперты используют в своей терминологии все больше термин, расширяющий права, — «пострадавший» вместо «жертвы». Следовательно, в этом отчете мы будем использовать оба термина.

- читать сообщения в мессенджере, независимо от того, используется ли шифрование;
- контролировать активность в социальных сетях;
- просматривать фотографии и видео;
- включать камеру.

Вся эта приватная информация может быть собрана с планшета или с любого смартфона.

Некоммерческие организации, входящие в Коалицию против сталкерского ПО, сообщают об увеличении числа пострадавших, обращающихся за помощью в связи с проблемой.

Некоммерческие организации, входящие в Коалицию против сталкерского ПО, сообщают об увеличении числа пострадавших, обращающихся за помощью в связи с проблемой:

- Результаты Второго национального исследования о злоупотреблении технологиями и насилии в семье в **Австралии**, проведенного WESNET при участии д-ра Делани Вудлок и исследователей из Университета Кертина, указывают, что среди 99,3% опрошенных жертв домашнего также подвергались кибернасилию при помощи технологий. Более того, в период с 2000 по 2015 год использование видеокамер увеличилось на 183,2%.
- Согласно исследованию о кибернасилии в отношениях, проведенного Centre Hubertine Auclert во **Франции**, 21% жертв сталкивался со сталкерским ПО, а 69% жертв считают, что их партнер скрыто получил доступ к персональным данным на их смартфоне.
- В **Германии** также на протяжении нескольких лет Women's Counselling Centers и Rape Crisis Centers (bff) отмечали рост использования сталкерского ПО в отношениях.
- В **США** по данным Центра по предотвращению сталкинга, информированию и ресурсам (SPARC) сталкинг затрагивает приблизительно 6–7,5 млн людей в год, одна из четырех жертв сообщает о преследовании с помощью технологий.

Ключ — физический доступ к устройству

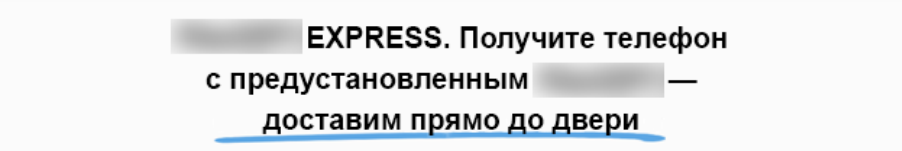
К сожалению, установить сталкерское ПО на телефон жертвы тайным образом не так трудно. Из-за особенностей вектора распространения таких приложений невозможно заразить устройство сталкерским ПО, например, через спам. Главным существующим барьером служит то, что сталкерское ПО должно быть установлено и настроено на устройстве.

Это означает, что у злоумышленника должен быть физический доступ к целевому устройству для установки сталкерского ПО. Это становится возможным, если устройство не защищено PIN-кодом, паролем или злоумышленник знает жертву лично. На установку может потребоваться несколько минут.

Перед получением доступа к устройству пострадавшего злоумышленник должен получить ссылку на пакет установки с веб-страницы разработчика сталкерского ПО. В большинстве случаев программное обеспечение не загружается из официального магазина приложений. Для устройств на Android компания Google запретила размещение приложений, которые явно являются сталкерским ПО, в своем магазине приложений Google Play в 2020 году. Это означает, что злоумышленник не сможет установить такое приложение из общего магазина приложений. Вместо этого злоумышленник должен выполнить несколько определённых шагов чтобы скачать и установить сталкерское ПО. Выполняя их злоумышленник «оставляет следы» в настройках устройства, по которым пользователь позже сможет проверить, установлено ли подобное ПО на его устройстве.

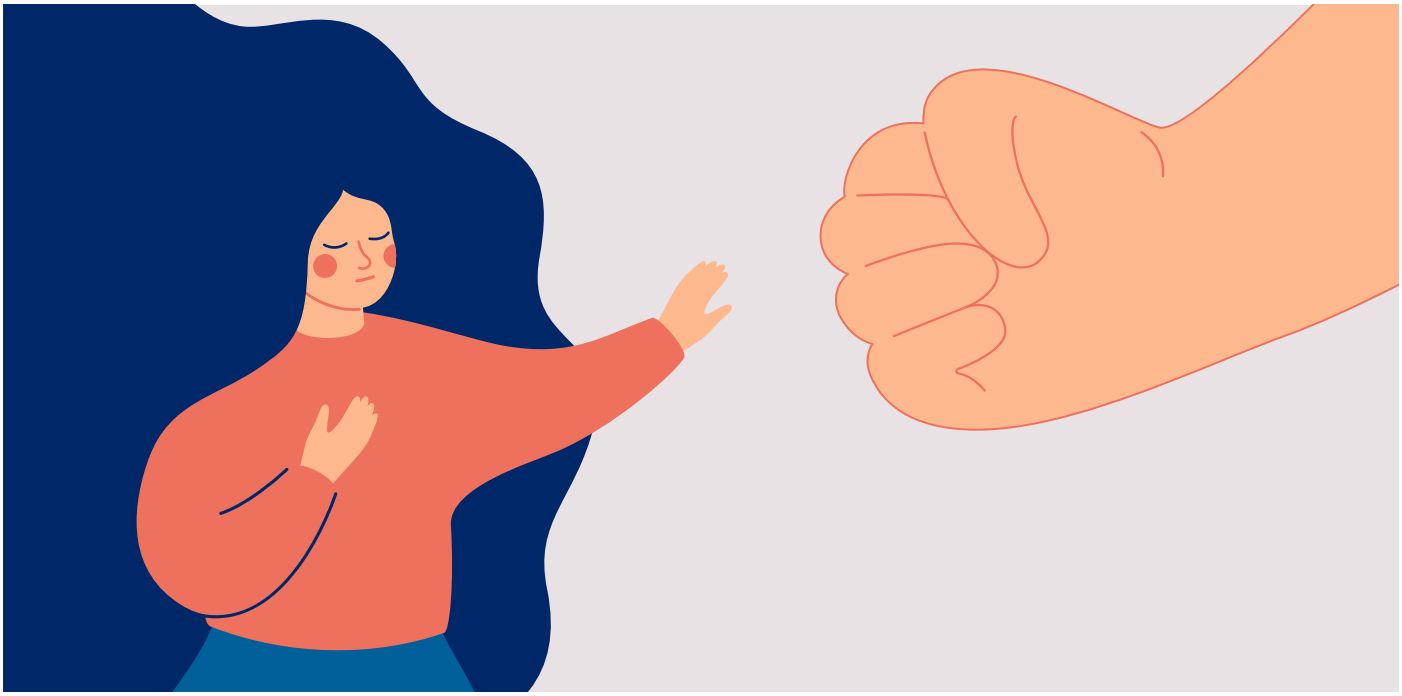
Сталкерское ПО встречается реже на iPhone, чем на устройствах на Android.

Сталкерское ПО встречается реже на iPhone, чем на устройствах на Android, потому что iOS — традиционно закрытая операционная система. Злоумышленники могут обойти это ограничение на взломанных iPhone, однако им все равно нужен физический доступ к телефону для его взлома. Таким образом, пользователи iPhone, которые боятся слежки за собой, должны всегда следить за своим устройством. Есть и другой способ: злоумышленник может подарить своей жертве iPhone или любое другое устройство с предварительно установленным сталкерским ПО. Есть много компаний, предлагающих онлайн свои услуги по установке таких инструментов на новый телефон и его доставку ничего не подозревающему адресату на праздник в качестве подарка.



Риск утечки конфиденциальной информации

Информация, контролируемая через сталкерское ПО, будет доступна по крайней мере одному человеку — злоумышленнику, установившему сталкерское ПО на телефон жертвы. Однако иногда случается и так, что все личные данные могут оказаться в открытом доступе. Из года в год серверы сталкерского ПО взламываются или остаются незащищенными от утечек. Например, в 2020 году такая утечка данных произошла из-за продукта, предоставленного ClevGuard. Ранее подобные инциденты были с Mobiispy в 2019 году и с MSpy в 2018 и 2015 году.



Это всего лишь несколько примеров из длинного списка, в котором базы данных компаний, разрабатывающих сталкерское ПО, попадали в открытый доступ, затрагивая миллионы учетных записей пользователей. Возможность отследить местоположение пользователя означает не только нарушение его киберконфиденциальности, но и риск для его безопасности в реальном мире.

Правовой статус

Сталкерские приложения продаются и предоставляются компаниями под различными прикрытиями, такими как решения для наблюдения за детьми или отслеживания сотрудников. Пока законы во всех странах различны, такие компании не сидят на месте. В целом, такие инструменты и приложения незаконно использовать только без согласия пользователя, на чье устройство по было установлено. Постепенно наблюдаются некоторые изменения в законодательстве по этому поводу. Например, в 2020 году Франция усилила санкции за тайный шпионаж: определение чьей-либо геолокации без согласия теперь наказуемо тюремным заключением на один год и штрафом в 45 000 евро. Если это совершено группой лиц, санкции могут быть выше — тюремное заключение на два года и штраф 60 000 евро.

Сталкерское ПО часто нарушает законы и влечет для сталкера правовую ответственность за любые записи, сделанные без ведома жертвы. Сталкеры должны понимать, что они нарушают закон. Если подается жалоба о незаконном использовании сталкерского ПО, наказание применяется к виновному, который установил программное обеспечение, а не к поставщику(продавцу) ПО. В новейшей истории США были оштрафованы только два разработчика таких приложений. Один из них должен был заплатить рекордный штраф в размере 500 000 долларов США, что положило конец процессу разработки приложений, а другой отделался распоряжением изменить функциональность приложения для продаж в будущем.

Масштаб проблемы

Всего 53 870 уникальных пользователей пострадали от сталкерского ПО в 2020 году во всем мире. В 2019 году мы обнаружили 66 927 уникальных пользователей.

Количество обнаружений во всем мире — пострадавшие пользователи

В этом разделе мы рассмотрим количество уникальных пользователей во всем мире, на мобильных устройствах которых было обнаружено сталкерское ПО.

Данные 2020 года показывают, что ситуация со сталкерским ПО не сильно улучшилась: количество пострадавших пользователей все еще высоко. Всего 53 870 уникальных пользователей пострадали от сталкерского ПО в 2020 году во всем мире. В 2019 году во всем мире пострадали 66 927 уникальных пользователей. Однако нужно учитывать тот факт, что 2020-й был беспрецедентным годом, когда жизнь людей по всему миру изменилась кардинально.

В рамках борьбы с пандемией COVID-19 все страны в мире столкнулись со значительными ограничениями, такими как меры по самоизоляции или карантину, призванные заставить людей оставаться дома. Учитывая то, что сталкерское ПО используется в качестве еще одного инструмента для контроля над партнером, с которым живет злоумышленник, это может объяснить некоторое снижение по сравнению с предыдущим годом.

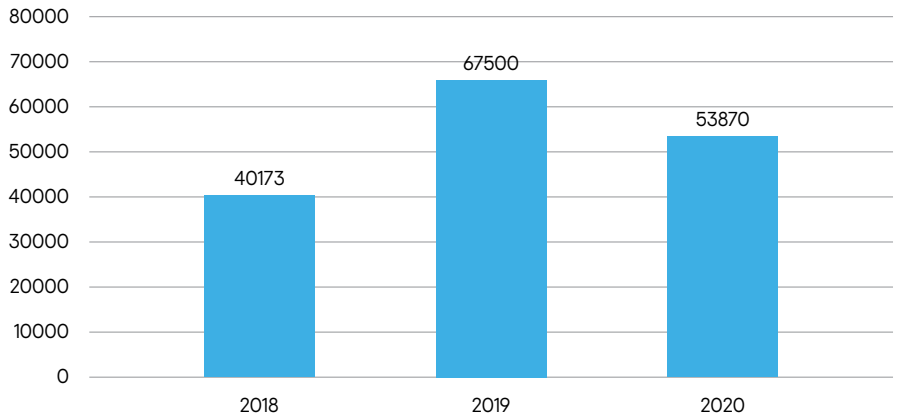


Таблица 1. Уникальные пользователи, пострадавшие от сталкерского ПО во всем мире с 2018 по 2020 год, общее количество за год.

Исходя из этого, показатели 2020 года находятся все еще на высоком стабильном уровне. Например, всего два года назад, в 2018 году мы выявили 40 173 уникальных пользователей, пострадавших от сталкерского ПО во всем мире.

Общее количество уникальных пользователей во всем мире, пострадавших от сталкерского ПО в 2020 году по месяцам, свидетельствует, что эта тенденция становится все более заметной. Первые два месяца года были стабильно высокими — это показывает, что сталкерское ПО было довольно популярным. Ситуация изменилась в марте, когда многие страны решили объявить о карантинных мерах. График показывает, что общее количество затронутых пользователей начало снижаться до показателей июня 2020 года — как раз в июне многие страны начали снимать ограничения.

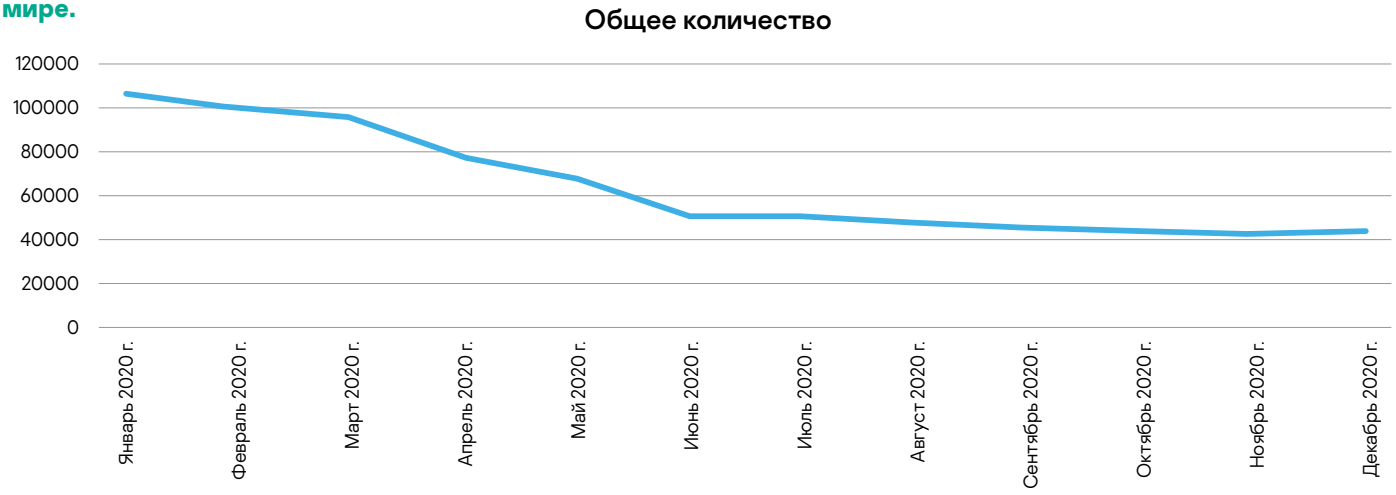


Таблица 2. Уникальные пользователи, пострадавшие от сталкерского ПО во всем мире в 2020 году, общее количество за месяц.

Исходя из этого, показатели 2020 года находятся все еще на высоком стабильном уровне. Например, всего два года назад, в 2018 году мы выявили 40 173 уникальных пользователей, пострадавших от сталкерского ПО во всем мире. К сожалению, это

означает, что программное обеспечение, используемое для шпионажа, становится все более распространенным видом насилия между партнерами.

Количество обнаружений во всем мире — образцы сталкерского ПО

В этом разделе мы проанализируем, какие образцы сталкерского ПО наиболее часто используются для контроля над мобильными устройствами на глобальном уровне. В 2020 году наиболее часто обнаруживаемыми образцами стали:

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

Таблица 3. 10 наиболее часто обнаруживаемых образцов сталкерского ПО в 2020 году по всему миру.

1. **Nidb** был наиболее используемым образцом сталкерского ПО в 2020 году, так как от него пострадало больше 8 100 пользователей. Создатель Nidb продает свое сталкерское ПО как услугу. Это означает, что любой человек может «арендовать» их сервер или приложение, переименовать их в любое удобное маркетинговое название и продавать их отдельно — этому уже есть примеры, включающие iSpyoo, TheTruthSpy, Copy9 и другие.
2. Второе и восьмое места занимает Cerberus. Это два различных образца из одного семейства. От варианта **Cerberus.a** пострадало больше 5 400 пользователей.
3. **Agent.af** занимает третье место с более чем 2 700 пострадавшими пользователями. Он продается под именем Track My Phone и обладает типичными функциями, такими как чтение сообщений, запись истории вызовов и отслеживание геолокации.
4. **Anlost.a** — хороший пример замаскированного сталкерского ПО. Оно рекламируется как приложение для защиты от кражи, и его значок присутствует на главном экране (необычное поведение для скрытых сталкерских приложений). Поэтому оно доступно в магазине приложений Google Play. Тем не менее можно сознательно скрыть значок на главном экране. Одна из ключевых функций приложения — перехват SMS-сообщений и чтение журнала вызовов. От этого образца пострадали более чем 2 200 пользователей.
5. **MobileTracker.c** имеет несколько функций, таких как перехват сообщений из популярных социальных сетей и дистанционное управление устройством. От этого образца пострадали более чем 2 100 пользователей.
6. **PhoneSpy** также известно как приложение Spy Phone или Spapp Monitoring. Это приложение обладает многими шпионскими функциями, охватывая все популярные службы мгновенных сообщений и социальные сети.
7. **Agent.hb** — это другая версия MobileTracker. Она, как и исходная версия, предлагает множество функций.
8. **Cerberus.b** — другой образец из того же семейства, что и Cerberus.a.
9. **Reptilic.a** — сталкерское ПО, которое включает много функций, таких как контроль социальных сетей, запись вызовов и контроль истории браузера.
10. **SecretCam.a** — это программное обеспечение для сталкинга с камерой, то есть оно может тайно записывать видео с передней или задней камеры устройства.

Географическое распространение пострадавших пользователей

Сталкерское ПО — это глобальный феномен, который затрагивает страны независимо от размера, типа общества или культуры. Если проанализировать 10 наиболее пострадавших стран во всем мире в 2020 году, результаты исследования «Лаборатории Касперского» показывают, что в основном наиболее затронутыми остаются те же страны во главе с Россией. Все же мы видим увеличение активности сталкерского ПО в Бразилии и США в 2020 году по сравнению с 2019-м. В то же время, мы обнаружили меньше инцидентов в Индии, которая снизилась в рейтинге. Мы также обнаружили рост количества затронутых пользователей в Мексике, которая повысилась в рейтинге на два места.

	Страна	Пострадавшие пользователи
1	Российская Федерация	12389
2	Бразилия	6523
3	США	4745
4	Индия	4627
5	Мексика	1570
6	Германия	1547
7	Иран	1345
8	Италия	1144
9	Великобритания	1009
10	Саудовская Аравия	968

Таблица 4. 10 наиболее пострадавших от сталкерского ПО стран в 2020 году по всему миру.

Что касается Европы, Германия, Италия и Великобритания стали тремя наиболее пострадавшими странами в указанном порядке. За ними следует Франция на четвертом месте и Испания на пятом.

	Страна	Пострадавшие пользователи
1	Германия	1547
2	Италия	1144
3	Великобритания	1009
4	Франция	904
5	Испания	873
6	Польша	444
7	Нидерланды	321
8	Румыния	222
9	Бельгия	180
10	Австрия	153

Таблица 5. 10 наиболее пострадавших от сталкерского ПО стран Европы в 2020 году.

Как проверить, установлено ли сталкерское ПО на мобильном устройстве

Обычному пользователю трудно определить, установлено ли сталкерское ПО на его устройстве. Обычно этот тип программного обеспечения пытается скрыть свое присутствие — скрывает иконку приложения на главном экране и в меню телефона и даже стирает любые оставленные следы. Существуют некоторые признаки, предупреждающие о его присутствии на устройстве. Вот самые важные из них:

- Обратите внимание на быструю разрядку батареи, постоянный перегрев и рост передаваемых мобильных данных.
- Регулярно проводите антивирусное сканирование своего устройства на Android: если решение для обеспечения информационной безопасности обнаружит сталкерское ПО, **не спешите удалять его, так как злоумышленник может получить оповещение об этом**. Тщательно обдумайте план обеспечения своей безопасности и обратитесь в локальную организацию по оказанию помощи.
- Проверьте историю браузера: для загрузки сталкерского ПО злоумышленник должен был посещать определенные веб-страницы, о которых пострадавший пользователь ничего не знает. С другой стороны, истории может не быть вообще, если злоумышленник стер ее.
- Проверьте галочку «Сторонние источники» (unknown sources): если она включена на вашем устройстве, это может быть признаком того, что нежелательное программное обеспечение было установлено из стороннего источника.
- Проверьте разрешения для установленных приложений: сталкерское приложение может быть замаскировано под другим именем с подозрительным доступом к сообщениям, журналу вызовов, определению местоположения и другой личной информации.

В то же время, важно понимать, что данные признаки необязательно являются доказательством того, что сталкерское ПО установлено на устройстве.

Как минимизировать риски

При насилии в семье и оскорбительных отношениях может быть трудно или даже невозможно запретить партнеру-злоумышленнику доступ к телефону.

Вот несколько советов, которые могут помочь повысить вашу безопасность в цифровом мире:

- Никогда не оставляйте телефон разблокированным и не давайте свой телефон другим людям. Особенно, если вы не будете видеть то, что этот человек делает на вашем телефоне*
- Используйте сложные пароли блокировки экрана и регулярно их меняйте.
- Не рассказывайте свой пароль никому — даже вашему партнеру, членам семьи или близким друзьям.*
- Регулярно проводите проверки своего телефона — удаляйте неиспользуемые приложения и проверяйте разрешения, выданные каждому приложению.
- Отключите параметр установки приложений из сторонних источников на устройствах на Android.
- Защитите свои устройства на Android с помощью защитного решения, такого как Kaspersky Internet Security for Android (бесплатное), которое обнаруживает сталкерское ПО и оповещает об этом.

* При насилии в семье и оскорбительных отношениях может быть трудно или даже невозможно запретить партнеру-злоумышленнику доступ к телефону.

Вклад «Лаборатории Касперского» в борьбу с кибернасилием

«Лаборатория Касперского» активно противодействует кибернасилию и использованию сталкерского ПО как отдельная компания, так и в сотрудничестве с многими другими партнерами. В 2019 году мы создали специальное оповещение, которое уведомляет пользователей, если сталкерское ПО установлено на их телефонах. В том же году мы вместе с девятью другими членами-учредителями

создали Коалицию против сталкерского ПО. В 2020 году мы создали TinyCheck, бесплатный инструмент для обнаружения сталкерского ПО на мобильных устройствах специально для организаций, работающих с жертвами насилия в семье. TinyCheck можно скачать по адресу https://github.com/KasperskyLab/TinyCheck. С 2021 года мы являемся одним из пяти партнеров проекта в масштабах ЕС, нацеленного на борьбу с гендерным кибернасилием и сталкерским ПО, который называется DeStalk. Его поддерживает Европейская комиссия в рамках своей программы «Права, равенство и гражданство».

О Коалиции против сталкерского ПО

Коалиция против сталкерского ПО («CAS» или «Коалиция») является организацией, целью которой является противодействие злоупотреблению использования технологий, сталкингу и преследованию с помощью создания и использования сталкерского ПО. После создания в ноябре 2019 года в Коалицию против сталкерского ПО вступили еще 26 партнеров в течение первого года ее существования. В их число входят партнеры-учредители — Avira, Electronic Frontier Foundation, (European Network for the Work with Perpetrators of Domestic Violence), G DATA Cyber Defense, «Лаборатория Касперского», Malwarebytes, The National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape и WEISSER RING. Коалиция стремится объединить различные организации, чтобы активно противодействовать преступлениям, совершенным с помощью сталкерского ПО, и повысить осведомленность общественности об этой важной проблеме. Из-за высокой социальной значимости для пользователей во всем мире и периодически появляющихся новых вариантов сталкерского ПО Коалиция против сталкерского ПО открыта для новых партнеров и призывает к сотрудничеству. Более подробную информацию о Коалиции против сталкерского ПО см. на официальном веб-сайте www.stopstalkerware.org.