О состоянии **сталкерского ПО** в 2022 году

Coalition Against Stalkerware

kaspersky

Содержание

Основные итоги 2022 года

Ежегодные отчеты «Лаборатории Касперского» о состоянии сталкерского ПО показывают, сколько людей становятся жертвами цифрового сталкинга во всем мире. Сталкерское ПО – это коммерческие программы, которые злоумышленники могут незаметно установить на мобильное устройство жертвы. Это позволяет им следить за личной жизнью владельца устройства без его ведома.

Для загрузки и установки такой программы необходимо только подключение к интернету и физический доступ к смартфону. При этом злоумышленник получает доступ к личным данным жертвы, тем самым вторгаясь в ее частную жизнь. Сталкерские приложения могут собирать разную информацию о жертве, но чаще всего это данные о местоположении устройства, текстовые сообщения, чаты в социальных сетях, фотографии, история браузера и многое другое. Сталкерские программы работают в фоновом режиме: большинство жертв даже не догадываются, что кто-то следит за каждым их шагом.

В большинстве стран использование сталкерского ПО не запрещено законом, однако установка подобного приложения на чужое устройство без согласия его владельца незаконна и влечет юридическую ответственность. При этом нести ее будет правонарушитель, а не разработчик программы.

Наряду с некоторыми другими инструментами, сталкерские программы являются формой технологического насилия и нередко применяются в целях психологического насилия в отношениях. Однако это лишь часть серьезной проблемы. Вот почему «Лаборатория Касперского» сотрудничает с экспертами и организациями по борьбе с домашним насилием, оказывающими помощь пострадавшим, реализует корректирующие программы для агрессоров, а также взаимодействует с исследовательскими организациями и государственными структурами – мы делимся с партнерами своими знаниями и оказываем поддержку как специалистам, так и жертвам насилия.

Основная статистика за 2022 год

- **По данным «Лаборатории Касперского», в 2022 году со сталкерским ПО столкнулись 29 312 уникальных пользователей во всем мире.** Несмотря на то, что в последние годы мы наблюдали нисходящий тренд, общее число пострадавших пользователей в целом осталось на уровне 2021 года. Тенденции, наблюдаемые в сфере разработки сталкерских приложений в течение последних лет, позволяют сделать вывод о некоторой стабилизации. Важно отметить, что анализируемая статистика получена только на основании данных о пользователях решений «Лаборатории Касперского». Общее число пострадавших по всему миру может быть значительно больше. Кроме того, среди жертв есть и те, кто пользуется другими защитными решениями, и те, кто вообще не использует подобные продукты.
- **Полученные данные свидетельствуют об устойчивом росте числа сталкерских атак на протяжении всего 2022 года.** В среднем каждый месяц 3333 пользователя становились новыми жертвами шпионов. Регулярное обнаружение подобных атак говорит о том, что сталкинг становится хронической проблемой и требует пристального внимания общественности. По оценке Коалиции по борьбе со сталкерским ПО, ежегодное количество жертв во всем мире приближается к миллиону.
- По данным Kaspersky Security Network, ч**аще всего жертвами сталкеров становятся жители России, Бразилии и Индии**, но в целом это явление распространилось по всему миру. На региональном уровне наибольшее число пострадавших пользователей наблюдается в следующих странах:
  - Германия, Италия и Франция (Европа);
  - Иран, Турция и Саудовская Аравия (Ближний Восток и Африка);
  - Индия, Индонезия и Австралия (Азиатско-Тихоокеанский регион);
  - Бразилия, Мексика и Эквадор (Латинская Америка);
  - США (Северная Америка);
  - Российская Федерация, Казахстан и Беларусь (Восточная Европа (кроме стран Европейского союза), Россия и Центральная Азия).
- Независимо от региона, самым распространенным приложением для преследования является Reptilicus, от которого пострадало 4 065 пользователей.

Тенденции 2022 года, наблюдаемые «Лабораторией Касперского»

Пострадавшие пользователи – глобальные показатели

Пострадавшие пользователи – глобальные показатели

В этом разделе мы сравниваем статистику, собранную «Лабораторией Касперского» в 2022 году на глобальном и региональном уровнях, с аналогичными данными за прошлые годы. В 2022 году общее число уникальных пользователей, столкнувшихся со сталкерским ПО, составило 29 312 человек. На графике 1 показано, как это количество менялось из года в год начиная с 2018 г.

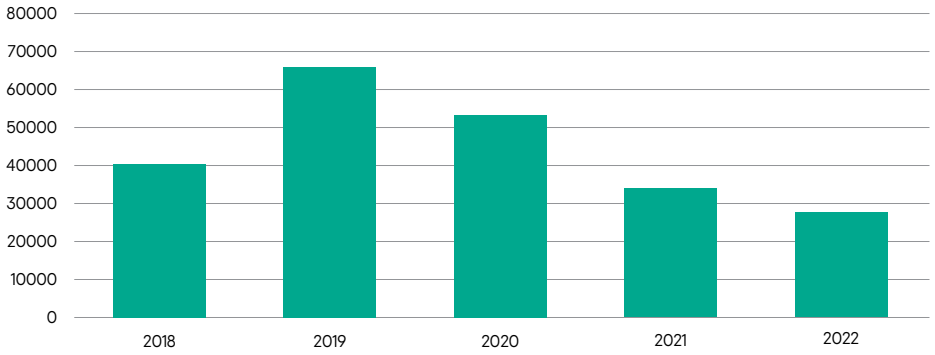


График 1. Изменение числа пострадавших пользователей по годам, 2018–2022 гг.

На графике 2 показано количество уникальных пострадавших пользователей в месяц в период с 2021 по 2022 год. Статистика 2022 года в целом осталась на уровне 2021 года, что говорит о стабилизации распространения сталкерского ПО. В среднем каждый месяц 3333 пользователя становились новыми жертвами сталкерского ПО.

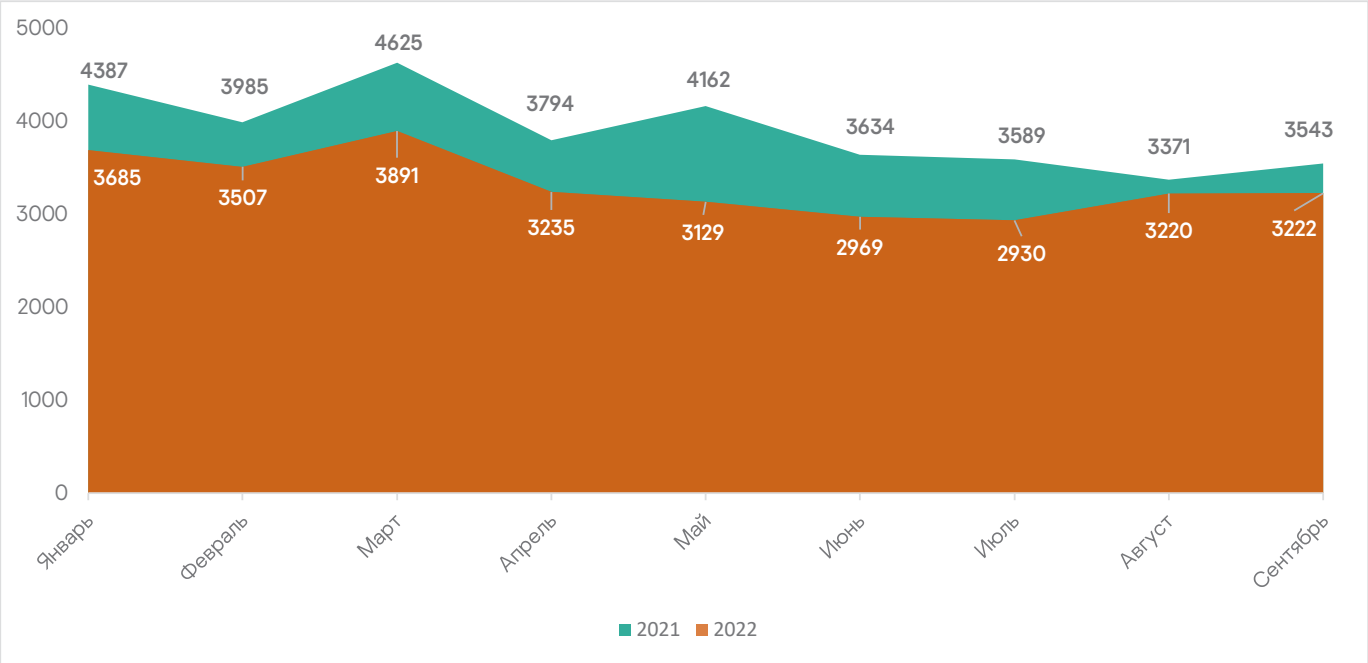
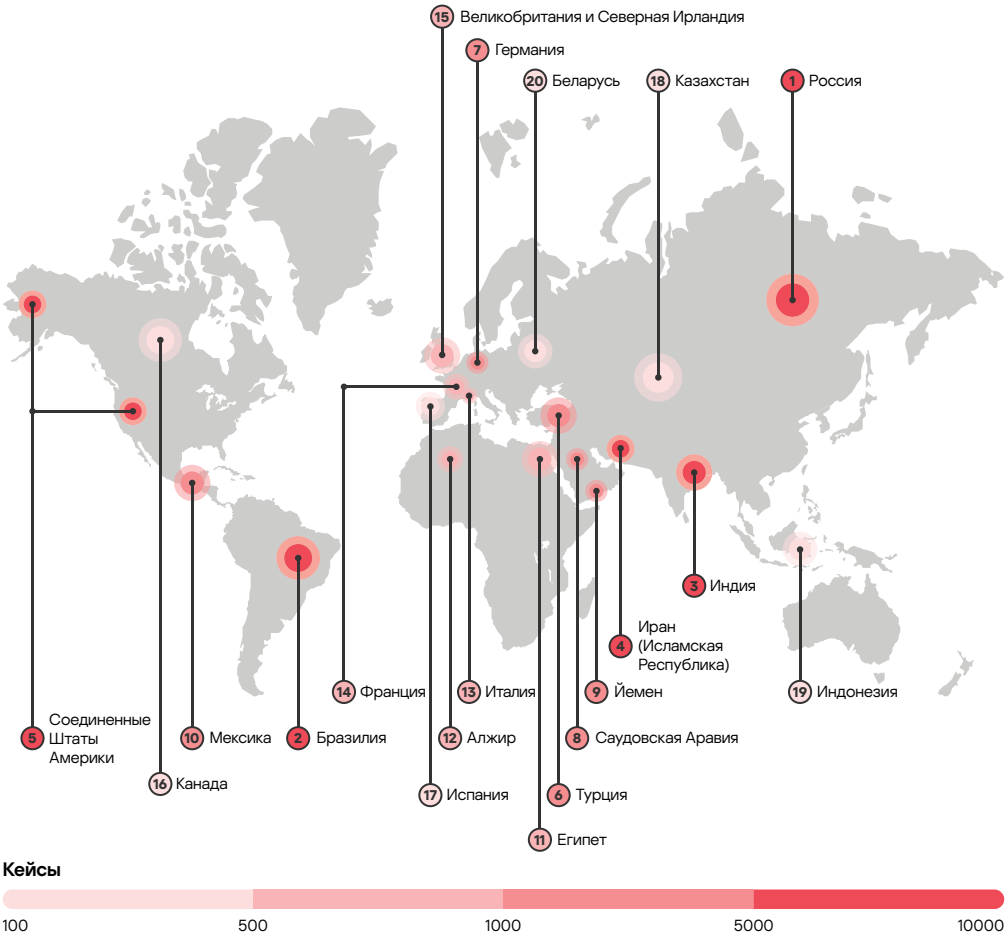


График 2. Число уникальных пострадавших пользователей в месяц в 2021–2022 гг.

География атак – глобальные и региональные показатели

Сталкерское ПО по-прежнему применяется во всем мире. По данным «Лаборатории Касперского», в 2022 году от него пострадали жители 176 стран.



Карта 1. Страны, лидирующие по числу сталкерских атак в 2022 году.

В 2022 году первые три места по количеству жертв заняли Россия (8281), Бразилия (4969) и Индия (1807). Эти три страны остаются бессменными лидерами рейтинга «Лаборатории Касперского» с 2019 года. В США количество пострадавших пользователей снизилось по сравнению с предыдущими годами и составило 1295 человек – сейчас эта страна занимает пятую строчку. В Иране, наоборот, наблюдался рост числа пострадавших – в 2022 году оно составило 1754 человека и вывело страну на четвертое место в рейтинге.

Однако, по сравнению с данными 2021 года, Иран стал единственной страной, впервые вошедшей в список и сразу оказавшейся в пятерке наиболее пострадавших. Россия, Бразилия, Индия и США входят в ТОП-5 уже не первый год. Турция, Германия и Мексика, как и в прошлом году, вошли в следующую пятерку самых пострадавших стран. В 2022 году к ним присоединились Саудовская Аравия и Йемен.

	Страна	Пострадавшие пользователи
1	Россия	8281
2	Бразилия	4969
3	Индия	1807
4	Иран	1754
5	Соединенные Штаты Америки	1295
6	Турция	755
7	Германия	736
8	Саудовская Аравия	612
9	Йемен	527
10	Мексика	474

Таблица 1. 10 стран, лидирующих в мире по числу сталкерских атак в 2022 году

Методология

В этом отчете используются данные по совокупной статистике угроз, полученные из сети Kaspersky Security Network. Kaspersky Security Network обрабатывает потоки данных о киберугрозах, полученных от миллионов добровольцев со всего мира. Все полученные сведения анонимны. Для расчета статистики мы проанализировали пользовательскую линейку решений «Лаборатории Касперского» для защиты мобильных устройств (согласно критериям обнаружения сталкерского ПО, разработанным Коалицией по борьбе со сталкерским ПО). Это означает, что число пострадавших пользователей включает только жертв сталкерского ПО. Другие типы мониторингового или шпионского ПО, которые не подпадают под определение Коалиции, не учитываются в текущей статистике.

Статистика отражает число уникальных пользователей мобильных устройств, пострадавших от сталкерского ПО. Оно отличается от общего количества обнаруженных случаев использования сталкерского ПО. Число обнаруженных случаев может быть еще больше, 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 данные о пользователях мобильных устройств с установленными защитными решениями «Лаборатории Касперского». Некоторые пользователи могут установить на свои устройства другое приложение, а некоторые вообще не используют подобные продукты.

В Европе общее количество уникальных пострадавших пользователей в 2022 году составило 3158 человек. Сталкерское ПО чаще всего применялось в Германии (737), Италии (405) и Франции (365). Страны, занявшие в этом списке с первого по седьмое место (Нидерланды), входили в ТОП-10 пострадавших европейских стран и в 2021 году. Новичками в этом рейтинге стали Швейцария, Австрия и Греция.

	Страна	Пострадавшие пользователи
1	Германия	736
2	Италия	405
3	Франция	365
4	Великобритания	313
5	Испания	296
6	Польша	220
7	Нидерланды	154
8	Швейцария	123
9	Австрия	71
10	Греция	70

Таблица 2. 10 стран, лидирующих в Европе по числу сталкерских атак в 2022 году

В Восточной Европе (за исключением стран Европейского союза), России и Центральной Азии общее количество уникальных пострадавших пользователей в 2022 году составило 9406 человек. В тройку лидеров вошли Россия, Казахстан и Беларусь.

	Страна	Пострадавшие пользователи
1	Россия	8281
2	Казахстан	296
3	Беларусь	267
4	Украина	258
5	Азербайджан	130
6	Узбекистан	76
7	Республика Молдова	34
8	Таджикистан	32
9	Киргизия	31
10	Армения	27

Таблица 3. 10 стран, лидирующих в Восточной Европе (кроме стран Европейского союза), России и Центральной Азии по числу сталкерских атак в 2022 году

В странах Ближнего Востока и Африки общее количество пострадавших пользователей составило 6330 человек, что незначительно превысило показатель 2021 года. В 2022 году Иран занял в этом списке первую строчку – количество пострадавших пользователей там составило 1754 человека. Турция поднялась на второе место в рейтинге по сравнению с прошлым годом (755 пострадавших пользователей). За ней следует Саудовская Аравия (612 пострадавших пользователей).

	Страна	Пострадавшие пользователи
1	Иран	1754
2	Турция	755
3	Саудовская Аравия	612
4	Йемен	527
5	Египет	469
6	Алжир	407
7	Марокко	168
8	Объединенные Арабские Эмираты	155
9	ЮАР	145
10	Кения	123

Таблица 4. 10 стран, лидирующих на Ближнем Востоке и в Африке по числу сталкерских атак в 2022 году

В Азиатско-Тихоокеанском регионе общее количество пострадавших пользователей составило 3187 человек. Индия существенно опережает другие страны, вошедшие в этот список: там насчитывается 1807 пострадавших. Второе и третье место заняли Индонезия (269 пострадавших пользователей) и Австралия (190 пострадавших пользователей).

	Страна	Пострадавшие пользователи
1	Индия	1807
2	Индонезия	269
3	Австралия	190
4	Филиппины	134
5	Малайзия	129
6	Вьетнам	109
7	Бангладеш	105
8	Япония	95
9	Таиланд	52
10	Пакистан	48

Таблица 5. 10 стран, лидирующих в Азиатско-Тихоокеанском регионе по числу сталкерских атак в 2022 году

В Латинской Америке и странах Карибского бассейна наибольшее число пострадавших пользователей (4969) зарегистрировано в Бразилии. Это приблизительно 32% от общего числа пострадавших пользователей в этом регионе. За Бразилией следуют Мексика и Эквадор, а Колумбия заняла четвертую строчку. Всего в регионе зарегистрировано 6170 пострадавших пользователей.

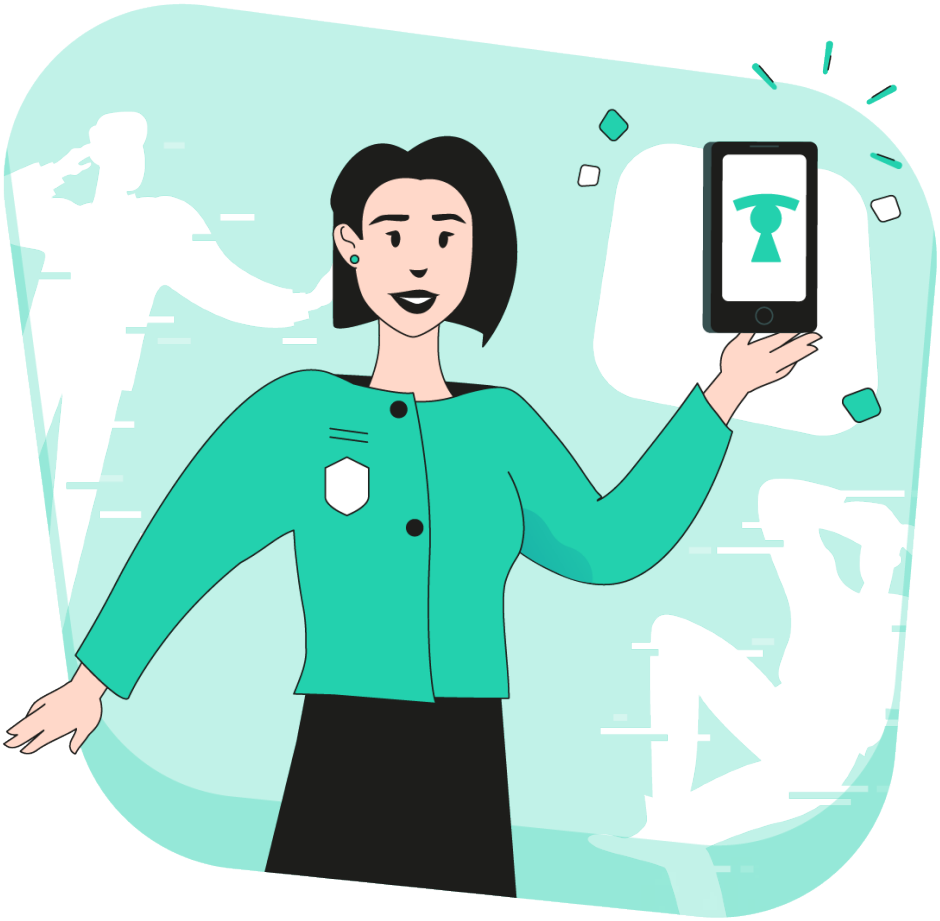
	Страна	Пострадавшие пользователи
1	Бразилия	4969
2	Мексика	474
3	Эквадор	146
4	Колумбия	120
5	Перу	111
6	Аргентина	85
7	Чили	49
8	Боливия	32
9	Венесуэла	30
10	Доминиканская Республика	24

Таблица 6. 10 стран, лидирующих в Латинской Америке по числу сталкерских атак в 2022 году

Наконец, в Северной Америке 87% всех пострадавших пользователей в регионе приходится на США. Это ожидаемые цифры, так как в этой стране проживает гораздо больше людей, чем в Канаде. В целом в Северной Америке пострадали 1585 пользователей.

	Страна	Пострадавшие пользователи
1	Соединенные Штаты Америки	1295
2	Канада	299

Таблица 7. Количество пользователей, пострадавших от действий сталкеров в Северной Америке в 2022 году



Сталкерские приложения – глобальные показатели

В этом разделе мы рассмотрим сталкерские приложения, которые чаще других используются для контроля мобильных устройств во всем мире. В 2022 году самым популярным приложением стало Reptilicus (4065 пострадавших пользователей). В этом году «Лаборатория Касперского» обнаружила 182 сталкерских приложения.

	Название приложения	Пострадавшие пользователи
1	Reptilicus (также Vkurse)	4065
2	Cerberus	2407
3	KeyLog	1721
4	MobileTracker	1633
5	wSpy	1342
6	SpyPhone	1211
7	Anlost	1189
8	Track My Phones	1137
9	MonitorMinor	864
10	Hovermon	827

Таблица 8. 10 самых популярных сталкерских приложений в 2022 году

Сталкерские программы позволяют следить за жизнью жертвы. Их функциональность варьируется в зависимости от типа приложения и от того, распространяется ли оно на платной основе или нет. Чаще всего сталкерские приложения распространяются под видом легитимного ПО предназначенного для защиты от кражи устройства или родительского контроля. На самом же деле они устанавливаются на смартфоны пользователей без их ведома и позволяют осуществлять слежку за жертвой в скрытом режиме.

В равной ли степени сталкерское ПО угрожает пользователям Android и iOS?

На устройствах iOS приложения сталкерского ПО встречаются реже, чем на устройствах Android, так как iOS традиционно является более закрытой системой. Злоумышленники могут обойти это ограничение на устройствах iPhone методами джейлбрейка. 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. В интернете есть много компаний, оказывающих подобные услуги. Таким образом агрессор может установить инструменты слежения на новый телефон и затем отправить его жертве в качестве подарка в заводской упаковке.

Вот несколько самых распространенных функций сталкерских программ:

- скрытие значка приложения;
- чтение SMS, MMS и журналов вызовов;
- получение списка контактов;
- 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 (в режиме селфи).

Цифровой сталкинг и гендерное насилие

Сталкерское ПО – это инструмент для кибersталкинга, который считается формой цифрового насилия.

Жертвами цифрового насилия могут стать как женщины, так и мужчины. Однако исследования показывают, что в подавляющем большинстве случаев насилию подвергаются именно женщины. Появление цифровых форм насилия заставляет нас взглянуть на этот феномен под новым углом. Онлайн-насилие следует рассматривать как продолжение физического насилия, поскольку его разрушительные последствия вполне реальны. Подробнее см. в докладе Cyber Violence against Women and Girls:Key Terms and Concepts (Кибернасилие в отношении женщин и девочек: основные термины и положения, 2022 г.), опубликованном Европейским институтом гендерного равенства.

Эксперты из академических кругов, а также некоммерческие организации, работающие со службами поддержки жертв и программами для правонарушителей, делятся с нами своим опытом и взглядами на цифровой сталкинг и злоупотребление технологиями в целом.

О важности данных для понимания масштабов цифрового насилия – доктор Леони Мария Танцер, доцент Университетского колледжа Лондона и руководитель исследовательской группы “Гендер и технологии”

Предыдущие исследования технологических форм преследования и гендерного насилия были посвящены ряду “повседневных” цифровых систем, которые могут использоваться, для принуждения, контроля и причинения вреда человеку или группе людей, в то время как текущий отчет и данные, рассматриваемые в нем, ограничиваются мобильными устройствами. При этом, необходимо помнить, что цифровой сталкинг может осуществляться с помощью различных устройств, включая GPS-трекеры или так называемый “Интернет вещей” (IoT). К последнему относятся продукты, подключенные к Интернету, такие как умные дверные звонки, камеры видеонаблюдения или колонки.

Доказательная база по случаям насилия с применением технологий также все еще очень ограничена. В настоящее время, большинство исследовательских центров находится в Австралии, Великобритании и США. Таким образом, большая часть исследований сосредоточена на данных, полученных из этих стран, что создает “белые пятна”. Данные, представленные в этом отчете, способствуют более широкому пониманию ландшафта технологического насилия, что крайне необходимо.

Кроме того, выяснилось, что службы поддержки жертв не успевают за технологическими достижениями. В результате чего существует острая необходимость дополнить существующие методы оценки рисков и обеспечения безопасности, включая “план действий по борьбе с кибersталкингом” и специальное обучение для повышения возможностей и оперативности сектора. И действительно, все чаще предлагаются специализированные услуги, как, например, команда Refuge по обеспечению технической безопасности, проект Safety Net Национальной сети по прекращению домашнего насилия (NNEDV) или клиника по прекращению технического насилия (CETA).

Исследовательская группа “Гендер и технологии” Университетского колледжа Лондона (UCL) изучает взаимосвязь между технологиями, безопасностью и гендером с целью сделать цифровые системы безопасными для всех. Узнайте больше: https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

Именно поэтому важно подчеркнуть опасность этого явления. Общество должно уделять больше внимания тем, кто страдает от цифрового насилия. С этой целью мы сотрудничаем с «Лабораторией Касперского» и другими партнерами Коалиции по борьбе со сталкерским ПО, оказывая поддержку жертвам и обеспечивая лучшую подготовку специалистов, работающих в сфере домашнего насилия.

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

Необходимо уделять больше внимания жертвам цифрового насилия – Елена Гаджотто, вице-президент итальянской неправительственной организации Una Casa Per L’Uomo

Кибersталкинг оказывает серьезное воздействие на жизнь тех, кто с ним сталкивается. Существуют средне- и долгосрочные психологические, физические и социальные последствия, которые мы ежедневно наблюдаем в наших центрах по борьбе с насилием. Как подчеркивает исследовательская служба Европейского парламента в своем исследовании (2021), любая женщина может стать потенциальной жертвой кибersталкинга, будь то общественный деятель, бывший партнер или просто пользователь социальных сетей. Кибersталкинг включает в себя различные типы поведения, такие как постоянные сообщения, наблюдение за деятельностью жертвы и другие формы преследования в сети, и, как говорится в том же исследовании, “не исключено, что кибersталкинг — это лишь дополнительный инструмент в арсенале злоумышленника”.

При работе с цифровым насилием необходимо учитывать следующие особенности:

- Цифровое насилие может осуществляться в сочетании с другими формами насилия (физическим, сексуальным, психологическим, экономическим и т.д.).
- Насилие может начаться в сети, а затем продолжиться в офлайн, или, наоборот, начаться в офлайн, а затем продолжиться в цифровой сфере.
- Навсегда удалить оскорбительный или провокационный контент, опубликованный в Интернете, очень непросто.
- Цифровое насилие может осуществляться как отдельными людьми, так и группами. Кроме того, злоумышленники не всегда могут быть известны жертве.
- Цифровое насилие может осуществляться с помощью широкого спектра устройств (ПК, смартфоны, умные домашние устройства и т.д.) и на различных платформах (веб-сайты, приложения для мгновенного обмена сообщениями, онлайн-чаты, социальные сети и т.д.).

Una Casa Per L’Uomo - итальянская неправительственная организация, предоставляющая услуги по поддержке жертв. Una Casa Per L’Uomo является членом Коалиции по борьбе со сталкерским ПО, а также партнером проекта DeStalk, который финансировался программой Европейского союза “Права, равенство и гражданство” и проходил в период с 2021 по 2023 гг.

Как уже было отмечено выше, несмотря на то что эти формы насилия осуществляются в киберпространстве, они оказывают серьезное влияние на реальную жизнь жертв. Исследования показывают, что в основном жертвами кибersталкинга или других форм цифрового насилия становятся женщины. Они испытывают практически те же симптомы, что и жертвы офлайн насилия, например, тревогу, панические атаки, посттравматический стресс, суицидальные мысли, гнев, неуверенность в себе и трудности с концентрацией внимания. Кроме того, возможны негативные экономические (вымогательство, потеря дохода и т.д.) и социальные (потеря семьи и друзей, социальная изоляция и т.д.) последствия. Помимо этого, цифровое насилие оказывает совокупное воздействие, как на экономическом, так и на политическом уровне: с одной стороны, увеличиваются государственные юридические, административные и медицинские расходы, а с другой - снижается участие женщин в общественном дискурсе.

Всеобщая борьба со сталкерскими программами

Прежде всего, следует помнить, что сталкерское ПО – это не техническая, а социальная проблема, для решения которой необходимо участие всех слоев общества. «Лаборатория Касперского» не только активно защищает пользователей от этой угрозы, но и работает над решением проблемы, сотрудничая с некоммерческими организациями, отраслевыми экспертами, исследовательскими компаниями и государственными учреждениями по всему миру.

В 2019 году «Лаборатория Касперского» первой в отрасли стала предупреждать пользователей своих решений о наличии сталкерского ПО на их устройствах. В то время как приложения «Лаборатории Касперского» уже много лет обнаруживают на устройствах потенциально опасные программы, не являющиеся вредоносными (в том числе сталкерское ПО), новое уведомление оповещает пользователей о наличии на их устройстве приложения, которое может следить за ними.

В 2022 году, в рамках запуска нового портфеля потребительских продуктов, «Лаборатория Касперского» расширила функции уведомления о нарушении конфиденциальности. Теперь пользователи получают предупреждение не только о наличии сталкерского ПО на устройстве, но и о том, что при его удалении установивший его человек узнает об этом, что может привести к обострению ситуации. Кроме того, удалив приложение, вы рискуете удалить и важные данные или доказательства, которые могут быть использованы правоохранительными органами при расследовании.

В 2019 году «Лаборатория Касперского» стала сооснователем Коалиции по борьбе со сталкерским ПО – международной рабочей группы по борьбе со сталкерскими программами и домашним насилием. Она объединяет усилия IT-компаний, НКО, исследовательских институтов и правоохранительных органов в области борьбы с кибersталкингом и помощи жертвам онлайн-насилия. Сегодня в состав Коалиции входят более 40 организаций, которые делятся друг с другом опытом и вместе работают над решением проблемы цифрового сталкинга. Пользователи, которые подозревают, что за ними следят через мобильное устройство, могут обратиться за помощью на сайте Коалиции, доступном на семи языках.

Coalition Against Stalkerware

С 2021 по 2023 гг. «Лаборатория Касперского» была партнером проекта DeStalk, запущенного в рамках программы EC Rights, Equality and Citizenship (Права, равенство и гражданственность). Проект объединил пять организаций-партнеров, а также экспертов по кибербезопасности, представителей исследовательских, общественных организаций и органов власти. В рамках проекта DeStalk обучение прошли 375 профессионалов, которые оказывают помощь пострадавшим женщинам и реализуют корректирующие программы для акторов насилия, а также представители органов власти. Они изучили эффективные методы борьбы со сталкерским ПО и другими формами цифрового гендерного насилия. Кроме того, в рамках этого проекта проводилась общественная работа по информированию населения о цифровом насилии и сталкерском ПО.

В рамках этого проекта «Лаборатория Касперского» разработала электронные учебные курсы по борьбе с кибернасилием и сталкерским ПО, которые доступны на бесплатной платформе Kaspersky Automated Security Awareness Platform на пяти языках в форме коротких занятий. Этот курс уже прошли 130 профессионалов, и еще 80 обучаются прямо сейчас. Несмотря на то, что проект DeStalk уже закрыт, электронный курс все еще доступен на сайте DeStalk https://www.work-with-perpetrators.eu/destalk.

В июне 2022 года «Лаборатория Касперского» запустила портал о TinyCheck – бесплатном и безопасном инструмент с открытым исходным кодом для некоммерческих организаций и отделов полиции, которые работают с жертвами цифрового сталкинга. С 2020 года он обнаруживает на устройствах пользователей сталкерское ПО и другие приложения для слежки незаметно для акторов насилия. Это независимое решение, которое не нужно устанавливать на пользовательское устройство: так преступник не узнает о факте проверки. TinyCheck подключается к устройству по сети Wi-Fi, анализирует исходящий трафик и обнаруживает случаи взаимодействия с известными источниками угрозы, например с серверами, обслуживающими сталкерское ПО. TinyCheck позволяет проверить любое устройство с любой операционной системой, в том числе с iOS и Android.

Подозреваете, что за вами шпионят? Вот несколько советов... ...

Независимо от того, подверглись ли вы атаке сталкера, советы помогут вам защититься от этой угрозы.

- Установите надежный пароль на свой телефон и не сообщайте его никому – даже родственникам, друзьям и коллегам.
- Периодически меняйте пароли всех своих учетных записей и храните их в тайне.
- Загружайте приложения только из официальных источников, например из Google Play или Apple App Store.
- Установите на свои устройства надежное защитное решение, например Kaspersky Internet Security для Android, и регулярно проверяйте их. Однако, если вы подозреваете, что программа для слежки уже установлена, сначала следует оценить все риски. Абьюзер может заметить, что вы используете решение кибербезопасности.

Жертвы сталкерского ПО могут подвергнуться и другим видам насилия, в том числе физическому.

В некоторых случаях злоумышленник может получать уведомления о том, что жертва проверяет устройство или удаляет приложение для слежки. Это может только усугубить ситуацию и вызвать еще большую агрессию. Вот почему важно действовать осторожно, если вы предполагаете, что за вами следят с помощью сталкерского ПО.

- **Обратитесь в местную службу поддержки.** Ближайшую к вам подобную организацию можно найти на сайте Коалиции по борьбе со сталкерским ПО.
- **Будьте внимательны, чтобы не пропустить признаки возможной атаки:** быстро разряжающийся аккумулятор (неизвестные или подозрительные приложения на устройстве могут потреблять много энергии) и недавно установленные приложения с подозрительными попытками доступа к информации о вашем местоположении, а также функциями отправки и получения текстовых сообщений или выполнения других подозрительных действий. Также проверьте, включена ли у вас функция «Неизвестные источники» (для устройств Android). Если да, то кто-то мог установить на ваше устройство нежелательные сторонние программы. Однако перечисленные выше признаки не всегда свидетельствуют о наличии сталкерского ПО на вашем устройстве и могут ничего не значить.
- **Не пытайтесь удалить сталкерское ПО, изменить его настройки или настройки телефона:** таким образом вы можете уведомить потенциального актора насилия и усугубить ситуацию. Кроме того, удалив приложение, вы рискуете удалить и важные данные или доказательства, которые могут быть использованы правоохранительными органами при расследовании.

Если вы хотите узнать больше о нашей работе по борьбе со сталкерским ПО или задать другой вопрос, напишите нам: 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/

TinyCheck:
https://tiny-check.com

Coalition Against Stalkerware

TinyCheck®

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