kaspersky активируй будущее


# Стилер-шторм: исследование рынка скомпрометированных учетных данных в даркнете

Что компаниям нужно знать об инфостилерах, и как от них защищаться

Kaspersky
Digital Footprint
Intelligence

Kaspersky
Digital Footprint
Intelligence

# Введение

Команда Kaspersky Digital Footprint Intelligence подготовила отчет на основе данных о миллионах устройств, скомпрометированных вредоносным ПО для кражи информации (инфостилерами).

**Инфостилер** — это вредоносное ПО, предназначенное для сбора и кражи конфиденциальной информации из системы: учетных записей и учетных данных, файлов cookie, данных кредитных карт, криптовалютных кошельков и так далее. Украденные данные передаются на C&C-сервер оператора вредоносного ПО с миллионов устройств по всему миру и собираются в лог-файлы, после чего распространяются в киберпреступном сообществе через даркнет-рынки.

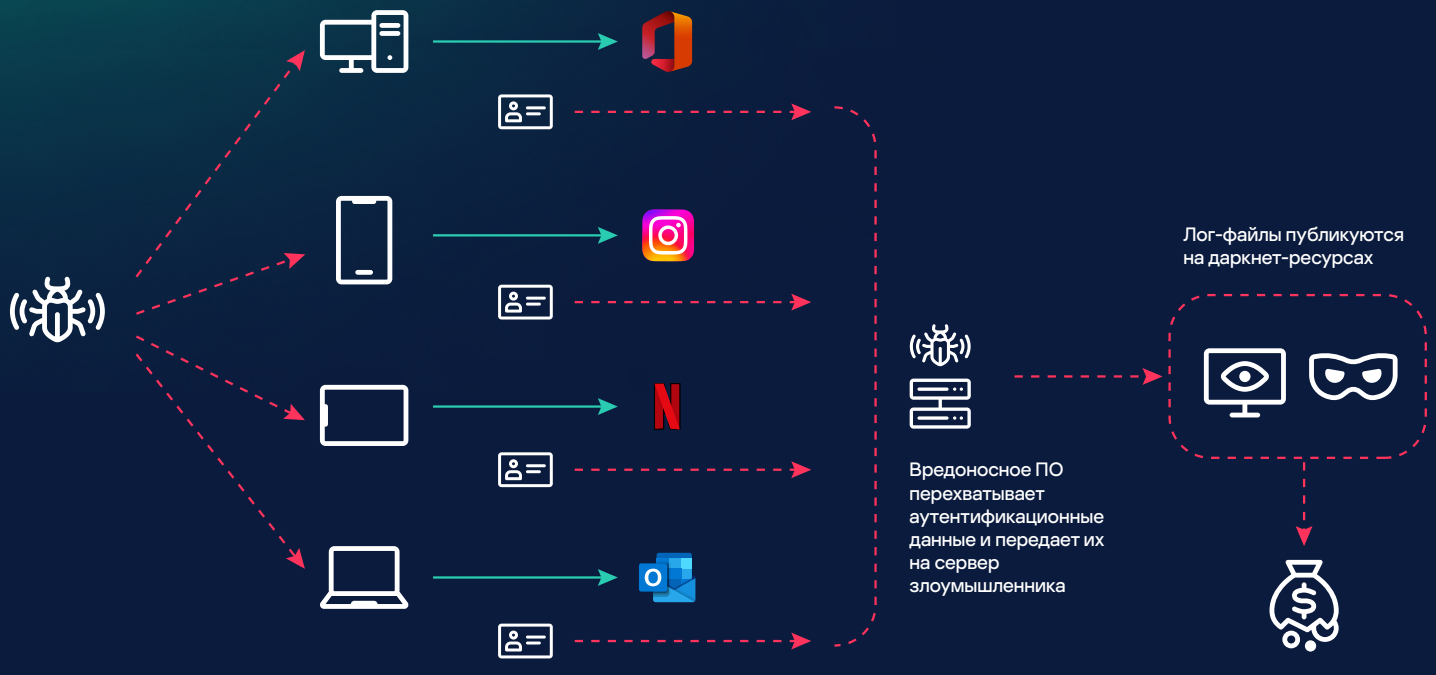
В этом отчете мы представляем статистику и главные выводы, основанные на обработке и анализе данных лог-файлов инфостилеров, собранных с 2021 по 2023 год.

# Источники информации для анализа

Киберпреступники публикуют лог-файлы, собранные инфостилерами с зараженных устройств, на закрытых ветках подпольных форумов. Эти файлы содержат учетные записи пользователя и другие его данные, а также информацию о скомпрометированном устройстве.

Обычно злоумышленники продают лог-файлы другим киберпреступникам, но могут делиться собранными данными и бесплатно. Например, если они уже извлекли необходимую информацию, то могут поделиться оставшейся, чтобы повысить свою репутацию в сообществе.

## Сценарий заражения устройства инфостилером



**50,9**

учетной записи в среднем содержит один файл

Мы анализируем лог-файлы, выделяя из них скомпрометированные учетные записи. Присутствие учетной записи пользователя в логах вредоносной программы (например, троянской программы или бота) указывает на то, что устройство этого пользователя было заражено.

Важно отметить, что один лог-файл соответствует одному заражению конкретной машины, но может содержать множество учетных записей от различных ресурсов, которые использовались на этом устройстве.

**на 35 %**

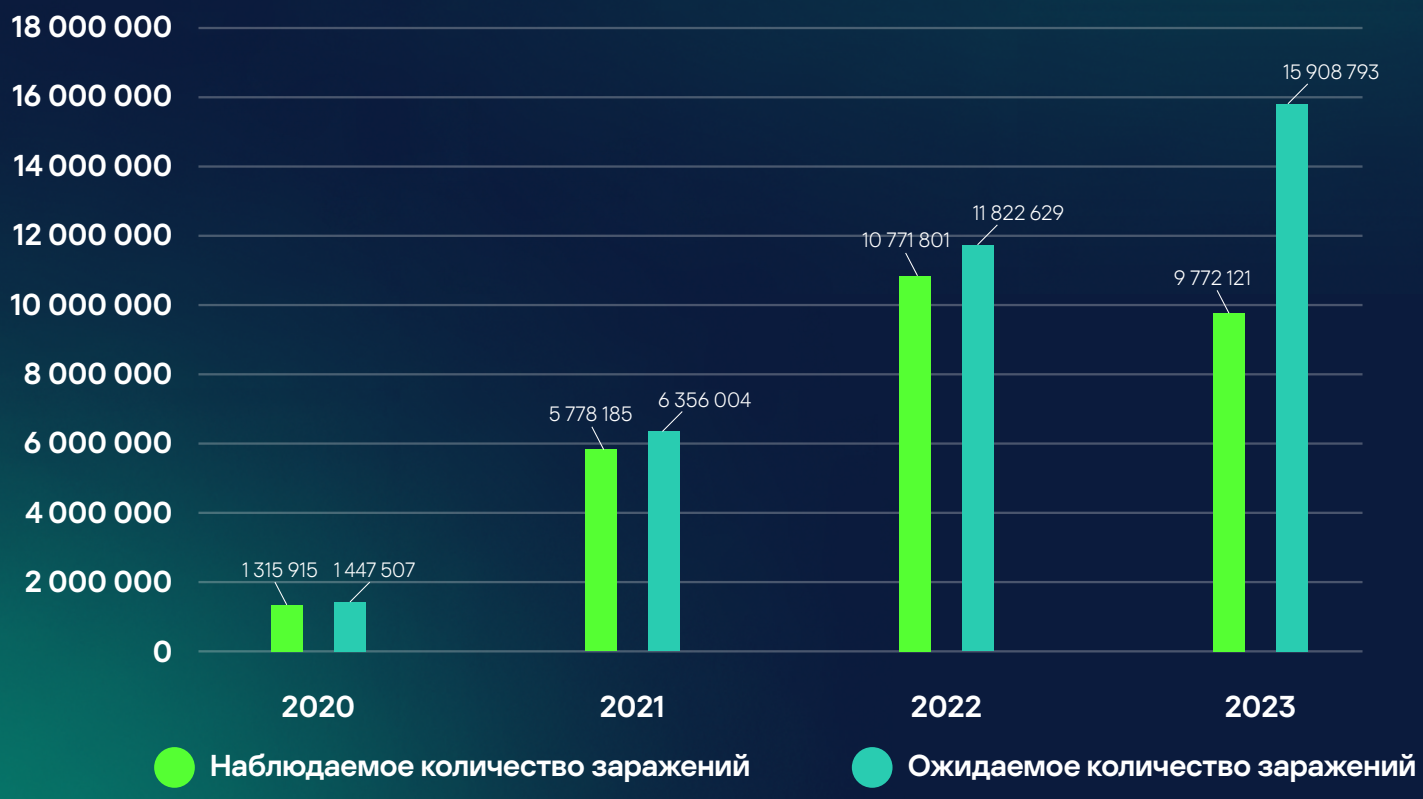
выросло количество обнаруженных заражений в 2023 году по сравнению с 2022 годом (на базе ожидаемого количества заражений). Дата заражения содержится в метаданных о скомпрометированных устройствах из лог-файлов инфостилеров

## Наблюдаемые тренды по заражениям

Следует учесть, что лог-файлы могут появляться в даркнете не сразу после компрометации. Например, учетная запись могла быть взломана в 2022 году, а соответствующий лог-файл опубликован только в 2023 году. Таким образом, справедливо будет ожидать дальнейшего роста фактического количества заражений за 2023 год с учетом прогноза числа тех лог-файлов, которые будут опубликованы в 2024 году.

На основе наблюдаемой динамики количества лог-файлов можно заключить, что в первые месяцы года показатель количества записей за предыдущий год больше, чем в последние месяцы года.

### Статистика по количеству заражений по годам




[1]Киберпреступники могут публиковать лог-файлы, содержащие скомпрометированные учетные записи, через месяцы или даже годы после заражения. Мы отслеживаем как даты публикации в даркнете, так и фактические даты компрометации. В 2024 году мы ожидаем увидеть больше данных, которые были скомпрометированы в 2023 году или ранее, но были опубликованы в даркнете некоторое время спустя. До 2022 года разница между наблюдаемыми и ожидаемыми случаями заражения меньше, поскольку большинство скомпрометированных учетных данных уже были опубликованы на различных даркнет-ресурсах.

Чтобы составить прогноз, мы сравнили количество скомпрометированных аккаунтов с 2020 по 2023 год по месяцам. Мы использовали эти данные для определения тренда, одновременно пополняя наши наборы данных за предыдущие годы. Это позволяет нам прогнозировать ожидаемое количество заражений с учетом предполагаемого объема данных, которые могут быть опубликованы в будущем.[1]

# Статистика заражений для различных ОС

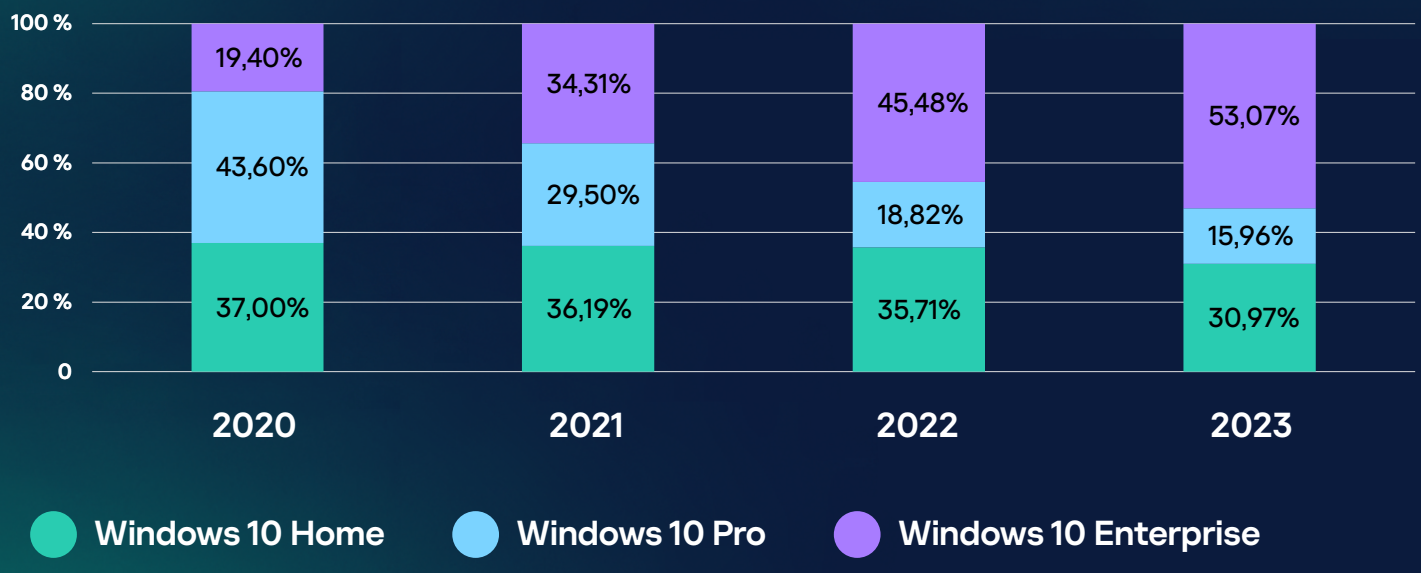
Судя по метаданным об устройствах из лог-файлов инфостилеров, основная часть скомпрометированных устройств работают на ОС Windows. Такая статистика объясняется в первую очередь общей популярностью данной ОС, а не проблемами с безопасностью: Windows — одна из самых распространенных операционных систем и в пользовательском, и в корпоративном сегментах.

Мы проанализировали статистику заражений для различных редакций этой ОС (Home, Pro, Enterprise). Эти данные позволяют выявить и разделить тенденции между корпоративными и индивидуальными пользователями.

## Статистика заражений по редакциям Windows 10

На диаграмме ниже отражено соотношение заражений между различными редакциями Windows 10, распределенное по годам с 2020 по 2023 год.

### Распределение заражений по затронутым версиям Windows 10 за 2020 - 2023

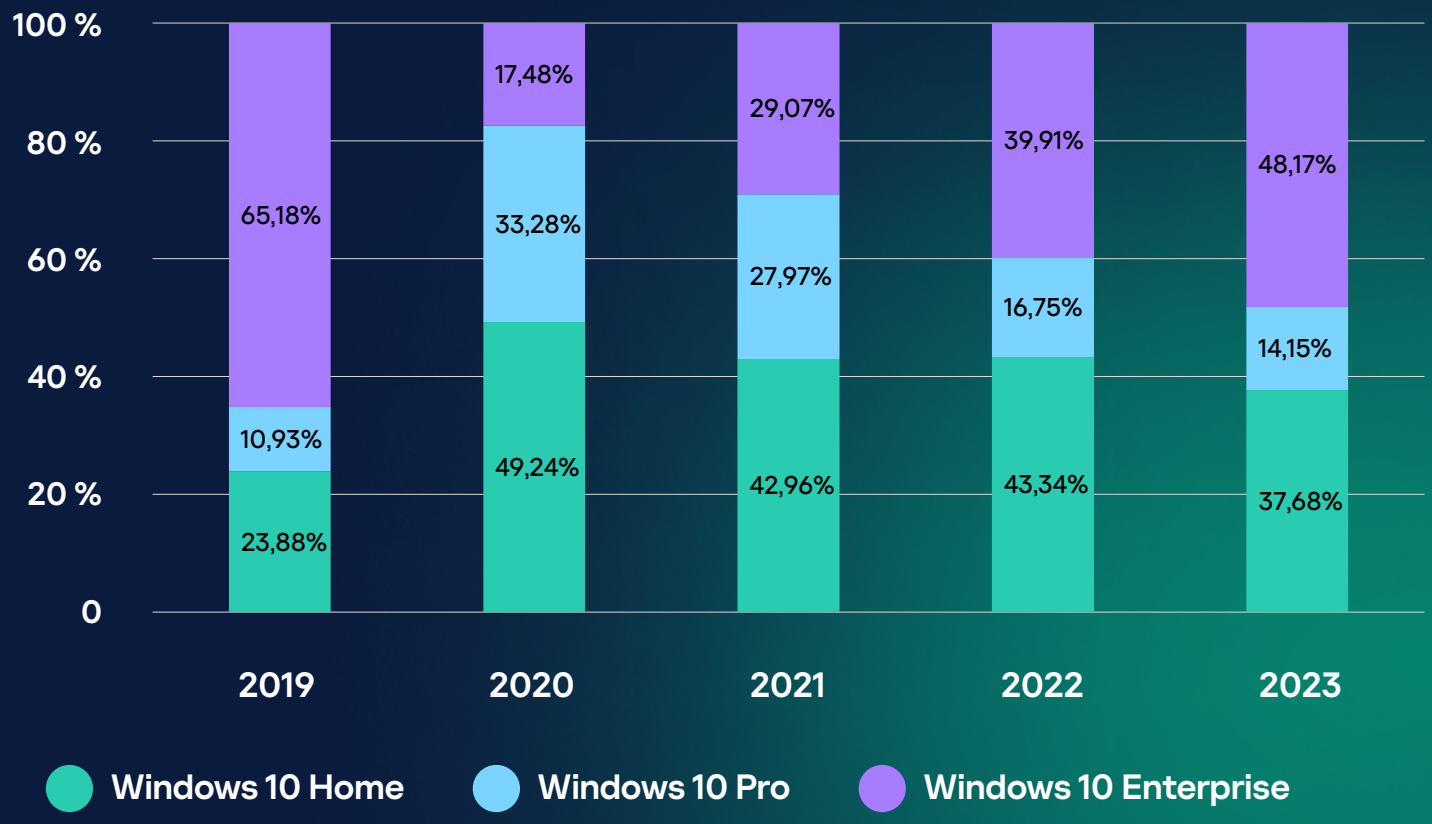



Из диаграммы видно, что количество скомпрометированных корпоративных пользователей в относительном выражении возрастает от года к году.

## Статистика по наличию корпоративных доступов в разрезе редакций Windows 10

Еще один тренд связан с компрометациями учетных записей с доступом к корпоративным ресурсам, встречаемых в различных редакциях Windows 10.

### Скомпрометированные корпоративные учетные записи в Windows 10




**В среднем в одном лог-файле злоумышленник может получить информацию об аккаунтах сотрудника с корпоративным электронным адресом в качестве логина к 1,85 веб-приложения**

На диаграмме видно, что количество учетных записей, обнаруженных в лог-файлах инфостилеров и связанных с редакцией Home, сократилось с 2020 года, и наибольшее число пришлось на тот же год.

Мы связываем эту тенденцию с пандемией COVID-19, которая началась в марте 2020 года и привела к массовому переходу сотрудников на удаленный формат работы (из дома) — зачастую с личных устройств.

На личных устройствах сотрудников обычно отсутствуют надежные меры безопасности, применяемые в корпоративных средах (такие как защитные решения, корпоративные и парольные политики). Данный фактор увеличивает вероятность успешного заражения устройства, потому что отсутствует дополнительный слой защиты, предотвращающий скачивание и запуск вредоносного ПО. Таким образом, компрометация личного устройства сотрудника, которое использовалось для доступа к рабочим ресурсам, может привести к утечке корпоративных учетных записей и доступов.

# Около 100

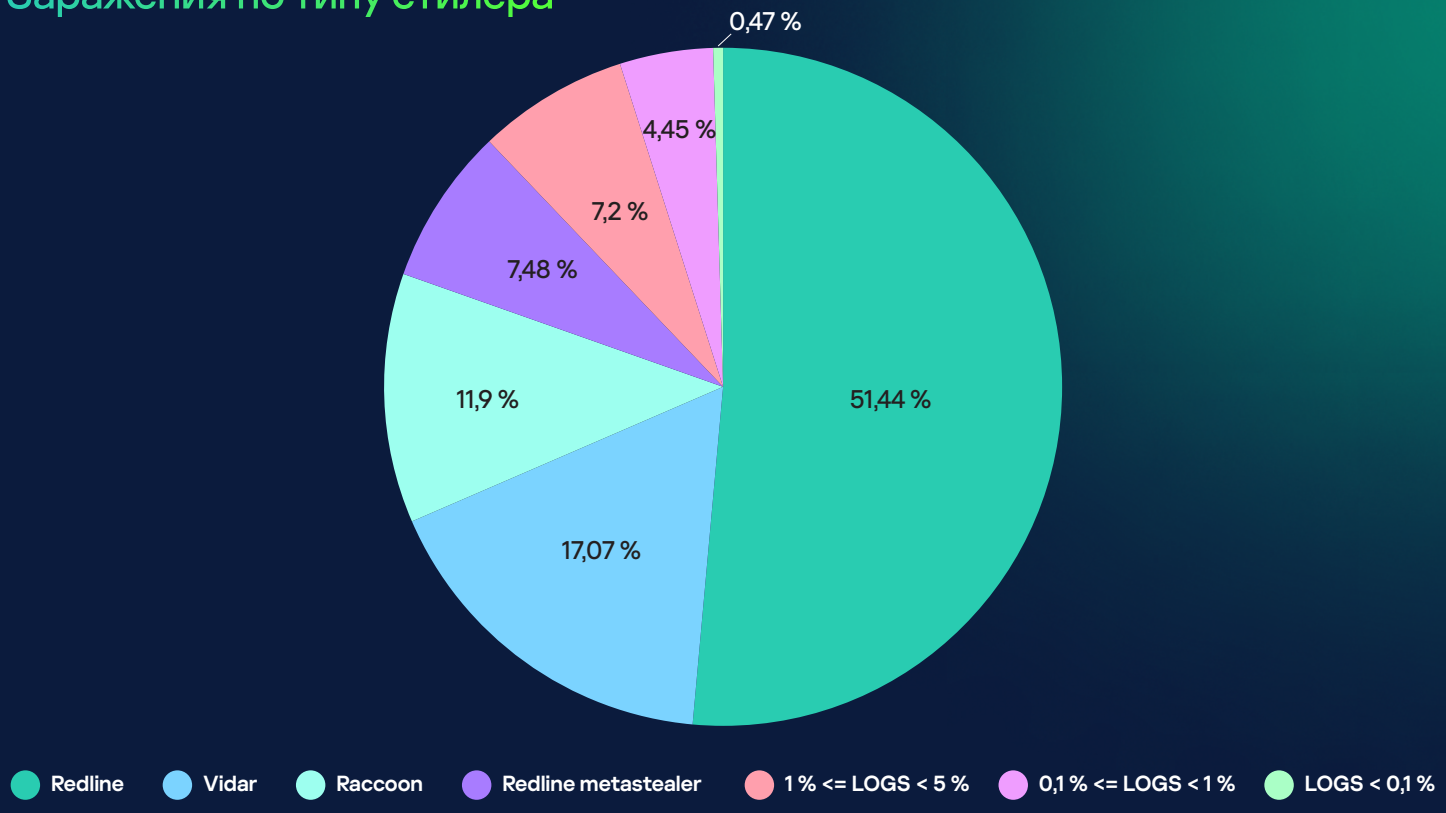
различных типов инфостилеров было обнаружено в лог-файлах[1].

[1] В зоне нашей видимости

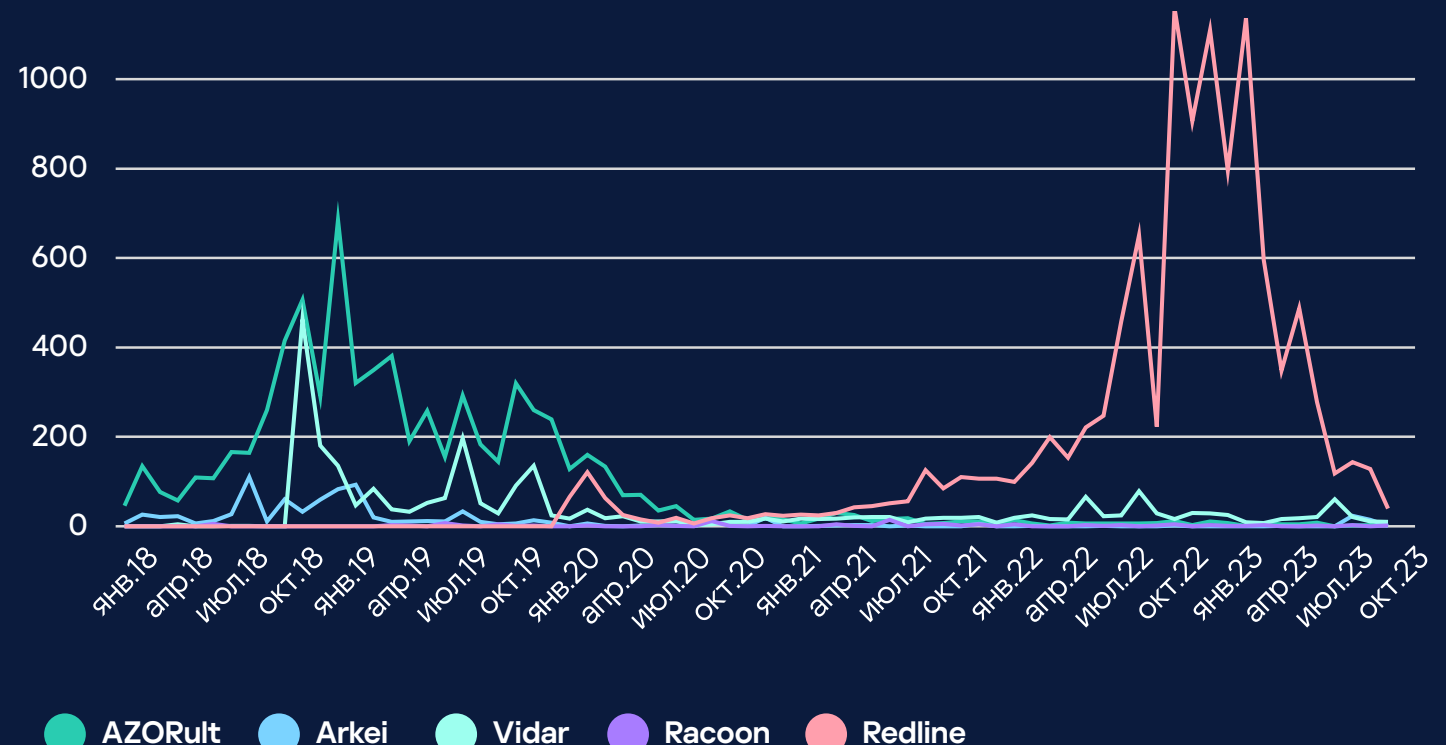
# Статистика заражений по типу стилера

На диаграмме ниже отражено процентное соотношение типов, которые мы выявили в 2020–2023 годах.

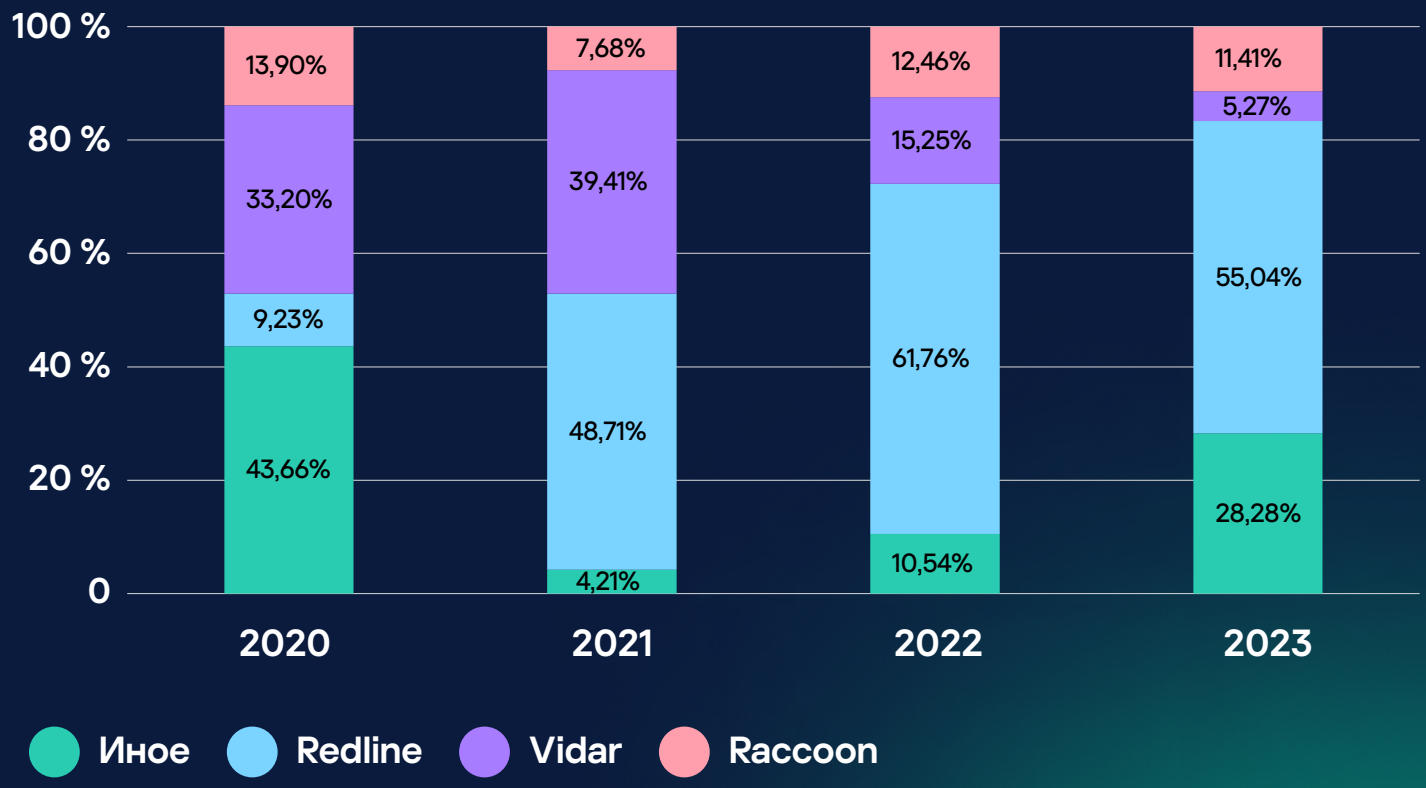
## Заражения по типу стилера




## Количество упоминаний различных стилеров на теневых форумах



Тенденции популярности трех наиболее распространенных стилеров за этот период выглядят следующим образом:




с 4,21%

до 28,28%

увеличилась доля заражений, приходящихся на новые виды стилеров, с 2021 по 2023 год

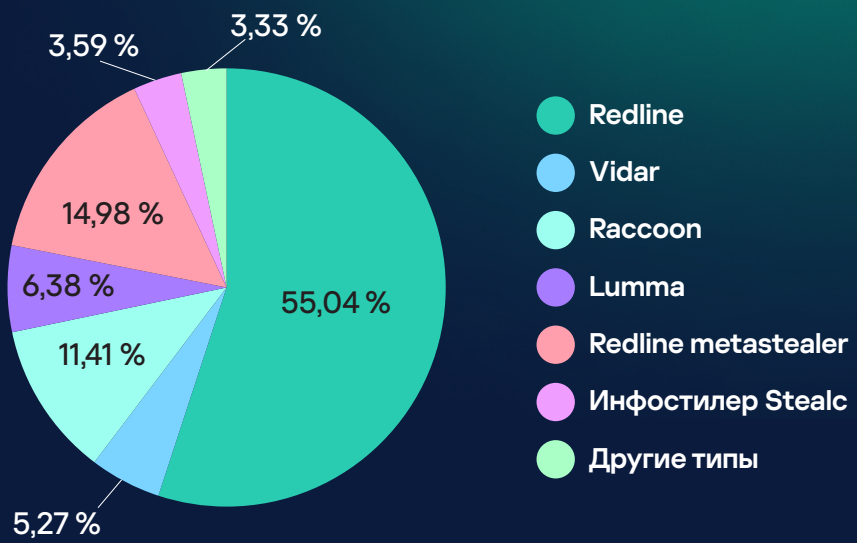
Подобная тенденция свидетельствует об активности на рынке разработки вредоносных решений.

Популярность стилера Redline возросла в 2021 году, и с тех пор около половины всех заражений стилерами приходится именно на него. Популярность стилера Vidar достигла пика в 2020 и 2021 годы, но ощутимо уменьшилась в последующие годы.

Стилер lumma, написанный на языке C, появился в конце 2022 года и стал набирать популярность в 2023 году за счет своей доступности по модели MaaS (Malware-as-a-Service). В основном он работает как обычный инфостилер, но имеет дополнительный фокус на криптокошельках. Заражение устройств осуществлялось с помощью обширных спам-кампаний через электронную почту, YouTube и Discord.

Среди новых стилеров также выделяется Stealc, на долю которого в 2023 году пришлось 3,59% заражений.

## Заражения по типу стилера, 2023




6,38%

заражений за 2023 год приходится на новый стилер lumma

# Статистика скомпрометированных учетных данных по доменам верхнего уровня

Мы проанализировали количество скомпрометированных учетных записей с сайтов, размещенных на различных региональных доменах. В выборке представлены домены верхнего уровня с латинскими буквами в именах и общие домены.

Ниже представлен список из 30 доменов с наибольшим в 2023 году количеством скомпрометированных учетных записей. На этих доменах количество случаев компрометации увеличилось в среднем на 230% по сравнению с 2021 годом.

Следует подчеркнуть, что некоторые домены используются для размещения не только локальных сайтов, но и популярных международных сервисов.

Например, стриминговая платформа Twitch использует домен .tv, являясь при этом международной платформой, не связанной с какой-либо конкретной страной. Этот факт может в значительной степени влиять на данные о частоте компрометации домена .tv, но на самом деле не обязательно коррелирует с уровнем угрозы инфостилеров в стране. В качестве дополнительных примеров можно указать такие сайты, как linked.in, telegra.ph и т. д. Фактически на любом домене могут размещаться популярные международные сайты, что делает такие домены привлекательной мишенью для киберпреступников. Важно понимать, что, хотя наличие таких сайтов в доменной зоне может влиять на данные о частоте компрометации учетных записей, оно не обязательно напрямую коррелирует с уровнем угрозы инфостилеров в стране, связанной с этим доменом.

| | Расширение домена верхнего уровня | Количество скомпрометированных учетных данных на домен, 2023 г.[1] |
|---|---|---|
| 1 | .com | 325 900 000 |
| 2 | .br | 28 800 000 |
| 3 | .in | 8 200 000 |
| 4 | .co | 6 000 000 |
| 5 | .vn | 5 500 000 |
| 6 | .io | 4 800 000 |
| 7 | .tv | 4 700 000 |
| 8 | .mx | 4 600 000 |
| 9 | .fr | 4 500 000 |
| 10 | .es | 4 400 000 |
| 11 | .id | 4 400 000 |
| 12 | .it | 4 200 000 |
| 13 | .ar | 4 200 000 |
| 14 | .tr | 3 800 000 |
| 15 | .pe | 3 400 000 |
| 16 | .cl | 2 900 000 |
| 17 | .pl | 2 700 000 |
| 18 | .eg | 2 700 000 |
| 19 | .de | 2 700 000 |
| 20 | .sa | 2 600 000 |
| 21 | .ru | 2 500 000 |
| 22 | .uk | 2 500 000 |
| 23 | .pk | 2 400 000 |
| 24 | .nz | 2 300 000 |
| 25 | .th | 2 200 000 |
| 26 | .me | 2 100 000 |
| 27 | .us | 2 100 000 |
| 28 | .hu | 2 000 000 |
| 29 | .bd | 1 600 000 |
| 30 | .eu | 1 600 000 |

[1] В таблице представлены округленные данные

# Анализ корпоративных систем

На основе собранных данных мы также собрали статистику по повторным заражениям корпоративных пользователей.

Мы выбрали 50 банковских организаций из различных регионов, для которых были проанализированы скомпрометированные учетные записи сотрудников[1]. Мы рассматривали крупные организации (1000 и более человек в штате), исключая те, в которых были выявлены единичные заражения.

Важно отметить, что рассматриваемые организации могут сильно отличаться между собой по набору услуг (страхование, лизинг, работа с юридическими лицами и так далее).

Мы выделили 3 категории повторных заражений:

1

**Краткосрочные — когда между повторными заражениями прошло менее 3 суток**

2

**Долгосрочные — когда между повторными заражениями прошло более 3 суток**

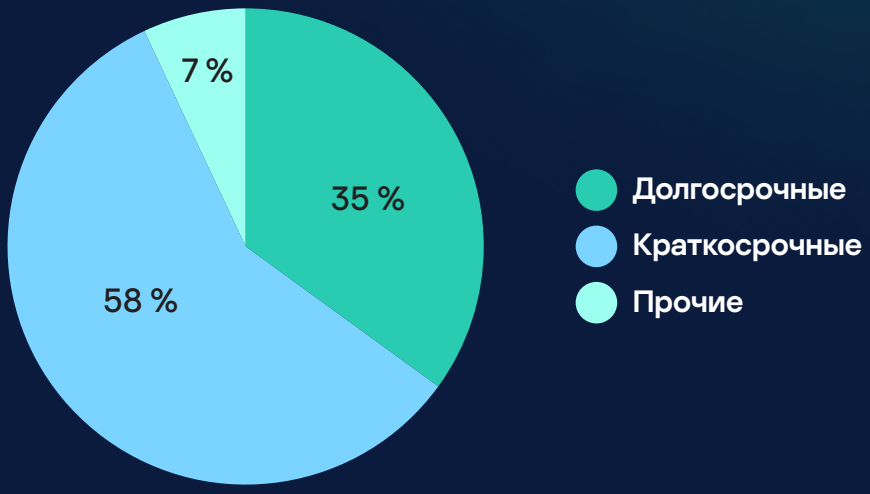
3

**Прочие — когда имеющаяся метаинформация не позволяет определить интервал между заражениями**

[1] В исследовании использовались адреса электронной почты из лог-файлов, обнаруженных в дарквебе и предположительно связанных с конкретными компаниями, попавшими в выборку. Скомпрометированные данные не проверялись, чтобы не допустить несанкционированного доступа к инфраструктуре компаний.

Согласно нашим данным, представленным на схеме ниже, большинство повторных заражений относится к краткосрочным и 35% — к долгосрочным.

## Повторные заражения




**Также мы можем сделать следующие выводы:**

**21,07%**

всех рассмотренных сотрудников, чьи устройства были заражены, запускали вредоносное ПО повторно

**8,94%**

зараженных сотрудников запускали вредоносное ПО **повторно спустя 3 и более суток** после первичного заражения

# Выводы и рекомендации

В последние три года мы наблюдаем постоянный рост количества заражений инфостилерами, попадающих в нашу зону видимости. Все больший процент скомпрометированных устройств приходится на систему Windows 10 Enterprise, что указывает на рост числа заражений корпоративных устройств.

Злоумышленники активно разрабатывают новые виды стилеров и применяют их в атаках. С 2021 по 2023 год более чем на 20% выросла доля устройств, для компрометации которых использовались варианты вредоносного ПО, не входящего в тройку самых популярных.

Мы также наблюдаем тенденции к повторному заражению устройств. Долгосрочные повторные заражения могут быть симптомами нескольких проблем:

**Недостаточный уровень осведомленности сотрудников**

**Недостаточно эффективные меры по обнаружению инцидентов и реагированию на них**

**Уверенность в том, что в случае компрометации учетной записи достаточно сменить пароль; отказ от детального разбора инцидента**

Компрометация учетных записей для сервисов представляет собой прямую угрозу безопасности пользовательских и иных данных, но сам факт заражения устройства уже указывает на возможную утечку конфиденциальных данных, которые на нем хранятся. Кроме того, в некоторых случаях злоумышленники могут сохранять доступ к зараженной машине в течение длительного времени.

Таким образом, при выявлении факта утечки данных через лог-файлы требуется предпринять следующие шаги для обеспечения безопасности:

- Незамедлительно сменить пароли для предположительно скомпрометированных учетных записей, проанализировать наличие подозрительных событий, связанных с данными учетными записями;
- Уведомить пользователей, чьи устройства могут быть заражены, о необходимости провести полную антивирусную проверку всех их устройств и удалить все обнаруженные вредоносные программы;
- Организовать проактивный мониторинг теневых площадок, чтобы выявлять скомпрометированные учётные записи до того, как они повлияют на кибербезопасность клиентов и сотрудников. Подробное руководство по настройке мониторинга можно найти **по ссылке**;
- Использовать сервис Kaspersky Digital Footprint Intelligence, чтобы быть в курсе того, что о ресурсах компании знают злоумышленники, и оперативно выявлять потенциальные векторы атак, а также своевременно настраивать необходимую защиту или принимать меры для устранения киберугроз.

Чтобы обеспечить эффективную защиту и снизить риски, связанные с заражением инфостилерами, рекомендуем выполнить следующие действия:

- Разработать программу повышения осведомленности в области информационной безопасности для сотрудников, обеспечить периодические тренинги и контроль эффективности по результатам обучения.
- Внедрить строгую парольную политику для всех корпоративных ресурсов.

**www.kaspersky.ru**