



Опыт  
международных  
экспертов  
помогает делать  
мир безопаснее

2020

# 2018

год основания компании

# 2019

запуск основного  
аналитического сервиса



Миссия Chronicle –  
помогать бизнесу в борьбе  
с киберпреступностью.

Входит в холдинг Alphabet  
(как часть Google Cloud)

## О клиенте

Компания Chronicle была основана холдингом Alphabet в 2018 году с целью предоставлять организациям и их сотрудникам инструменты для защиты критически важной инфраструктуры и систем от глобальной киберпреступности.

Компания задействует глобальные вычислительные мощности и аналитические возможности, позволяющие корпоративным службам безопасности выявлять киберугрозы прежде, чем системам будет причинен вред.



- Штаб-квартира в Маунтин-Вью, Калифорния
- Chronicle использует аналитические отчеты «Лаборатории Касперского» об АРТ-угрозах

## Вызовы



### Надежное партнерство

Глобальная сеть аналитиков мирового класса предоставляет компании Chronicle уникальную и актуальную информацию о киберугрозах

По оценкам аналитиков, доходы от киберпреступности превышают 1,5 трлн долларов США в год. Потенциальной мишенью является каждый гражданин, каждая организация и даже каждое государство.

По прогнозам, к 2031 году глобальный ущерб от действий программ-шифровальщиков будет достигать 250 млрд долларов США ежегодно<sup>1</sup>. Одна типичная **атака типа «отказ в обслуживании» (DoS)** **может обойтись крупному предприятию более чем в 2 млн долларов США**. Телефоны, компьютеры, автомобили, счета в банках и банковские карты, даже устройства для «умного дома» и системы сигнализации уязвимы к атакам киберпреступников.

Chronicle сотрудничает с крупными корпорациями и государственными органами, применяя обширный опыт анализа данных, чтобы помочь переломить ситуацию и остановить злоумышленников. В ее арсенале есть средства для сбора огромного количества телеметрических данных о безопасности организаций по всему миру и получения уникальной аналитической информации об актуальных глобальных угрозах. На основе этих инструментов создан комплексный аналитический сервис, помогающий нейтрализовать киберугрозы до того, как жертве будет нанесен ущерб.

Но Chronicle понимает, что в борьбе с киберпреступностью жизненно важно получать актуальную информацию о киберугрозах и том, как им противостоять.

<sup>1</sup> По данным Cybersecurity Ventures



Kaspersky  
Threat Intelligence

## Преимущества Kaspersky Threat Intelligence

- Актуальные данные о новых угрозах и уязвимостях, позволяя действовать на опережение
- Информация в реальном времени о возникающих угрозах и индикаторах компрометации
- Усилия существующие средства защиты, повышение эффективности обнаружения и предотвращения сложных атак
- Целостное представление о цифровых активах и выявляет наиболее уязвимые цели для атак

## Решение «Лаборатории Касперского»

**Сервис аналитических отчетов об АРТ-угрозах** (от англ. advanced persistent threat – комплексная целевая угроза), входящий в портфолио сервисов Kaspersky Threat Intelligence, опирается на работу команды глобального центра исследований и анализа угроз (GReAT). Деятельность команды получила признание во всем мире благодаря разоблачению ряда известных злоумышленников и раскрытию изощренных кампаний кибершпионажа.

Пользователи сервиса GReAT, анализирующего ландшафт АРТ-атак по всему миру, получают постоянный доступ к уникальным исследованиям и обнаруженным угрозам. Уведомления об инцидентах подкреплены подробными отчетами, содержащими индивидуальные практические советы и рекомендации, а также полные технические данные. Благодаря этой информации, организации могут быстро реагировать на новые угрозы и уязвимости: блокировать их, внедрять рабочие практики, уменьшающие потенциальный ущерб. Опираясь на отчеты GReAT, можно разрабатывать более эффективные стратегии цифровой безопасности.

Организациям также становится доступен полный архив отчетов «Лаборатории Касперского» об АРТ-угрозах. Этот уникальный ресурс предоставляет прекрасную возможность ознакомиться с уже изученными угрозами, извлечь уроки и укрепить знания и навыки сотрудников служб кибербезопасности.



Лаборатория Касперского» предлагает глубокие экспертные знания в сочетании с объемом телеметрии, который недоступен у других сервисов. При этом компании присущи такие черты, как любопытство и стремление узнавать новое – в частности, желание выявлять новые угрозы и прогнозировать их глобальные последствия. Это встречается крайне редко.

**Хуан Андрес Герреро Сааде (Juan Andres Guerrero Saade),**

Исследователь, Chronicle Security

## Глобальная платформа телеметрии

Основной сервис Chronicle представляет собой глобальную платформу телеметрии для анализа и поиска угроз в корпоративных сетях. Сервис построен на базовой инфраструктуре Google. Благодаря скорости и масштабируемости он позволяет быстро, безопасно и без лишних затрат управлять огромными объемами телеметрических данных по безопасности и анализировать их.

По словам исследователя Chronicle Хуана Андреса Герреро Сааде, поддержка «Лаборатории Касперского» обеспечивает жизненно важный дополнительный уровень информации и экспертных знаний об угрозах.

«Наши команды в Chronicle разбирают огромные объемы телеметрических данных, которые генерируют компании, чтобы решить, какие области действительно требуют внимания и подвергаются угрозам, а затем определить, как мы можем устраниить риски», – говорит он.

«Мы знали, что именно на такие вопросы должны помочь ответить сервисы Kaspersky Threat Intelligence. Специалисты «Лаборатории Касперского» предоставляют нам действительно ценную информацию о новых незнакомых нам угрозах, а не просто заваливают выжимками из новостей, которые не добавляют ничего нового к нашему пониманию.



Часто «Лаборатория Касперского» первой выявляет новую угрозу еще до того, как о ней узнают производители программного обеспечения. Возможность проконсультироваться с экспертом позволяет нам получить более полное представление об угрозе, оперативно спланировать ответные меры и наилучшим образом защитить наших клиентов»

**Хуан Андрес Герреро Сааде (Juan Andres Guerrero Saade),**

Исследователь, Chronicle Security



### Скорость

Мгновенно предоставляемая экспертами поддержка экономит время



### Надежность

Опыт всемирно признанных экспертов в области обнаружения новых киберугроз



### Уникальная ценность

Регулярное быстрое выявление новых угроз



### Эффективная аналитика и план действий

Отчеты об APT-угрозах содержат индикаторы компрометации и YARA-правила, а также практические советы и рекомендации



**Kaspersky  
Threat Intelligence**

Подробнее

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2025, АО «Лаборатория Касперского».  
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью  
их правообладателей.

#kaspersky  
#активируйбудущее