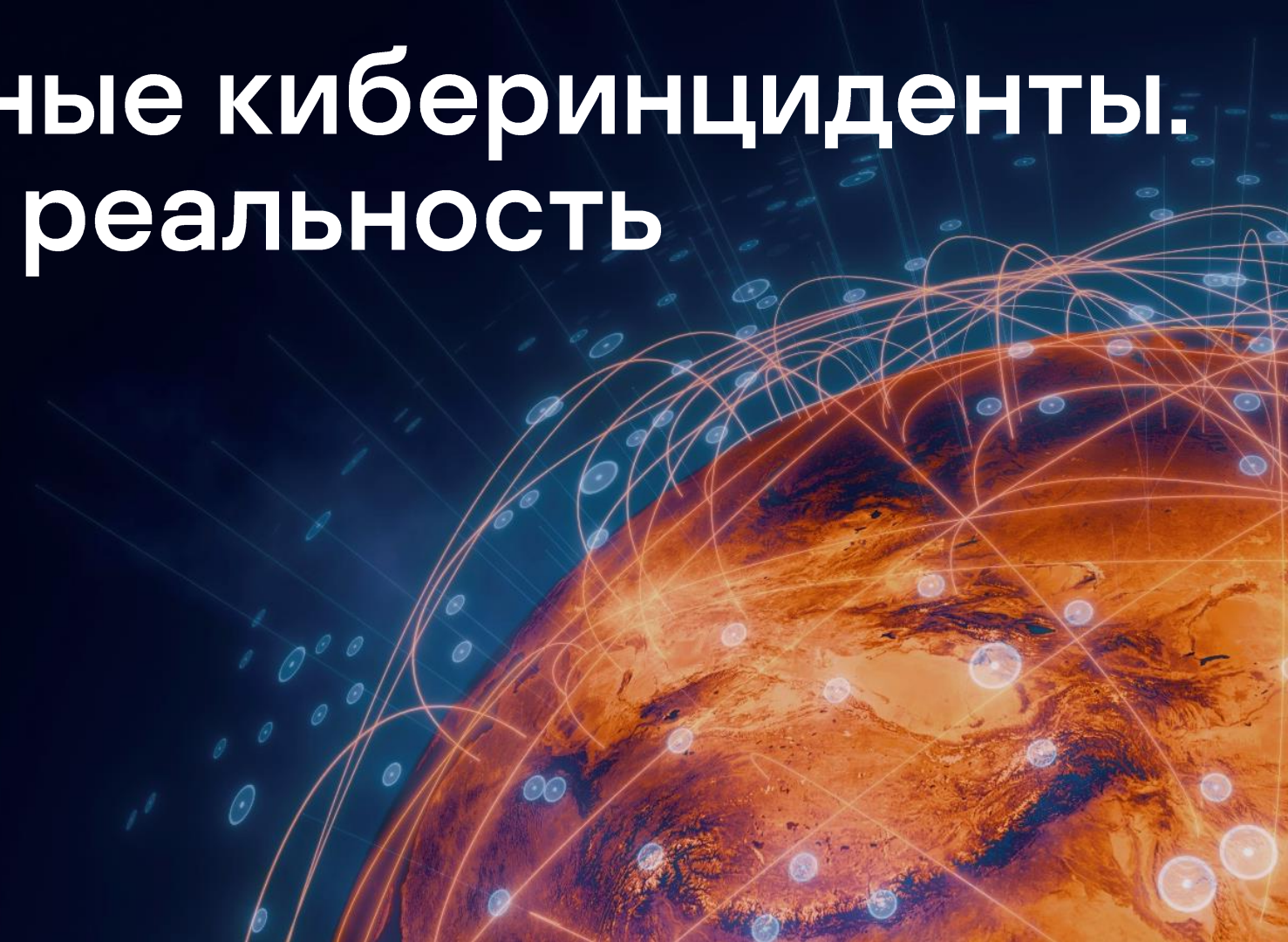
Сложные кибериниденты. Новая реальность



Алексей Шульмин,
вирусный эксперт

kaspersky BRING ON THE FUTURE

Высокоуровневый ландшафт угроз

360 000

уникальных вредоносных объектов мы обнаруживаем ежедневно

kaspersky

Общее число образцов в нашей вирусной коллекции превысило **1 млрд**

Высокоуровневый ландшафт киберугроз

kaspersky

Основные тренды

Трояны-вымогатели и ransomware 2.0

Сотрудничество APT и киберпреступников
Киберпреступники – начальный доступ

Продолжающаяся эксплуатация темы COVID-19

Киберпреступные группы соединяют силы

- Картели-вымогатели (например, Maze)
- Филиалы и подбор персонала (пр. REvil $1m депозит)
- Разделение труда (ransomware as service)

Эксплуатация «темных пятен»

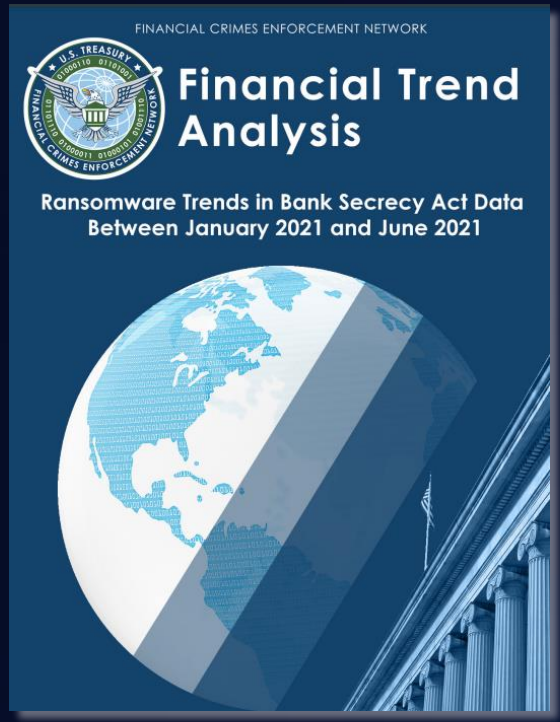
- Повышенный интерес к сетевой инфраструктуре
- Устаревшее оборудование/ПО – роутеры, VPN, (виртуальные) устройства

kaspersky

Масштаб проблемы

По данным US Treasury's Financial Crimes Enforcement Network (FinCEN):

Только в H1 2021 организации только из США заплатили более **600 млн долларов** вымогателям.



Совокупный объем средств, полученных наиболее успешными группами злоумышленников, за последние 3 года составил порядка **5,2 миллиардов долларов**.

kaspersky

https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

Ransomware 2.0

тренд 2019-2021

kaspersky

Ransomware до 2019

Автоматизированные массовые атаки как на бизнес, так и на обычных пользователей

Требование выкупа за расшифровку файлов

Контрмеры: антивирусная защита и регулярное резервное копирование

Ransomware 2.0

Полноценные целевые атаки на крупный и сверхкрупный бизнес (в т.ч. с оборотом > 10 млрд. $) с кражей конфиденциальных данных

Требование выкупа за расшифровку и отказ от публикации украденных данных

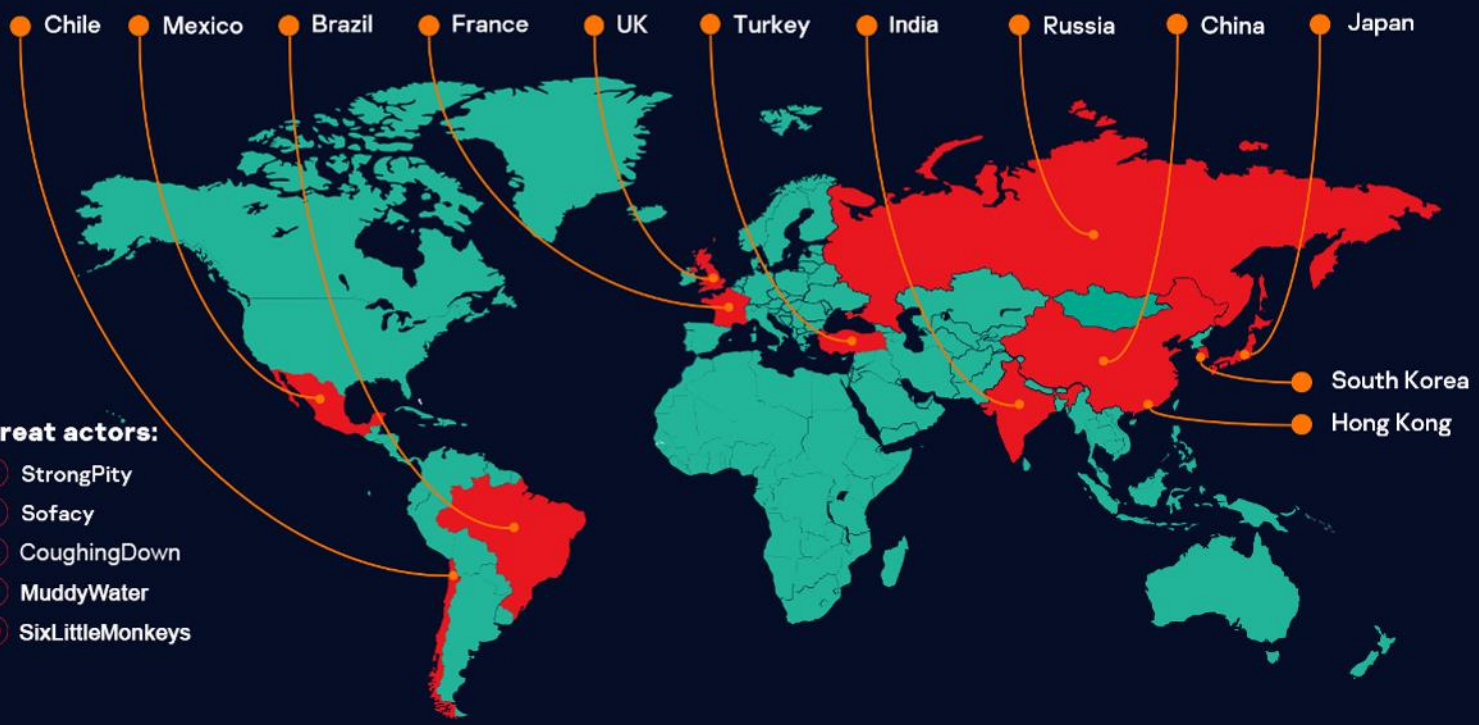
Контрмеры: комплексная защита организации от целевых атак

Ландшафт сложных таргетированных угроз

Top 10 targets:

- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries and territories:



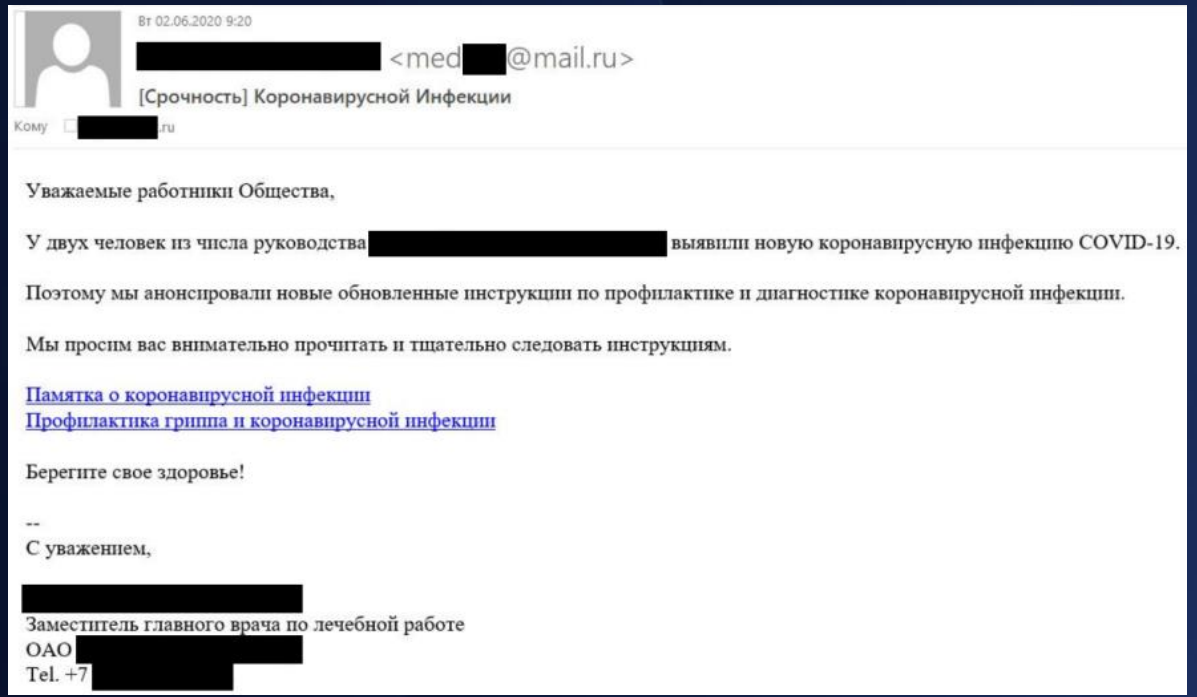
Top 10 significant threat actors:

1. Lazarus
2. DeathStalker
3. CactusPete
4. IAmTheKing
5. TransparentTribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixLittleMonkeys

apt.securelist.com

Lazarus

- **Использование тематики COVID**
- **Использование персональных данных сотрудников атакуемых организаций (собраны из общедоступных источников)**
- **2 варианта атаки:**
  1. **Документ с вредоносным макросом прикреплён к письму**
  2. **Письмо содержит ссылку на вредоносный документ**


Вт 02.06.2020 9:20
[redacted] <med[redacted]@mail.ru>
[Срочность] Коронавирусной Инфекции
Кому [redacted].ru

Уважаемые работники Общества,

У двух человек из числа руководства [redacted] выявили новую коронавирусную инфекцию COVID-19.

Поэтому мы анонсировали новые обновленные инструкции по профилактике и диагностике коронавирусной инфекции.

Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

Памятка о коронавирусной инфекции
Профилактика гриппа и коронавирусной инфекции

Берегите свое здоровье!

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

kaspersky

Lazarus

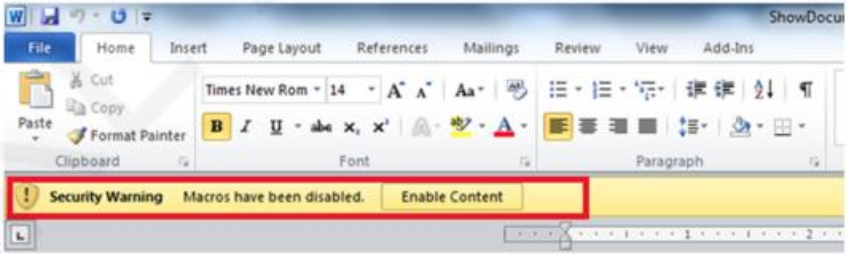
Чт 21.05.2020 12:22

[redacted]

Re[2]: Коронавирусной Инфекции

Кому [redacted]ru

Это зависит от совместимости просмотра документов.
Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно настроить содержимое.



FYI:

Если вы все еще не видите содержимое, я перешлю документ.

--
С уважением,

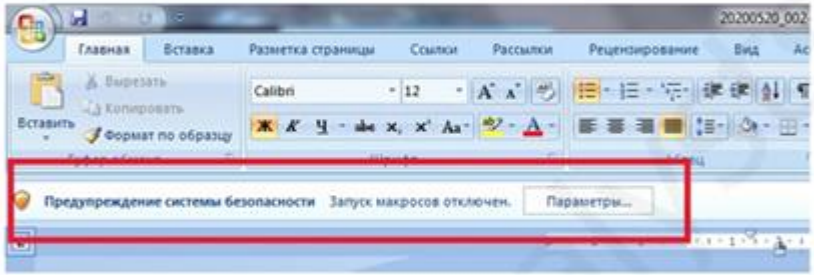
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

Чт 21.05.2020 12:36

[redacted]mail.ru>

Re[2]: Коронавирусной Инфекции

Кому [redacted]ru



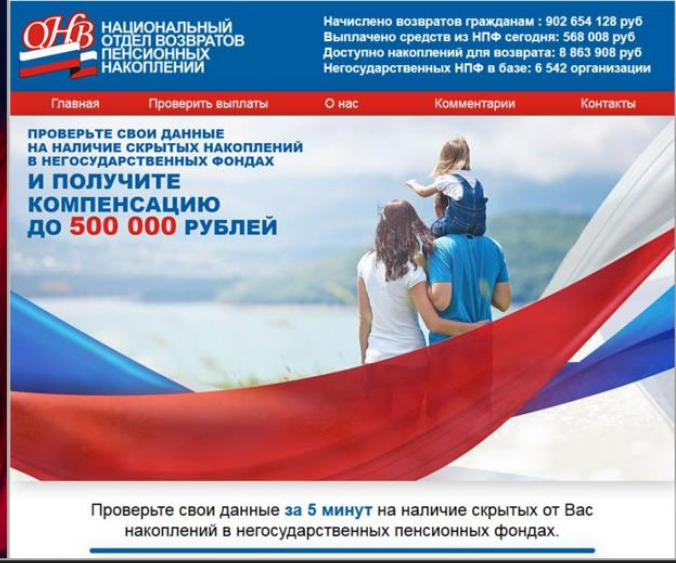
--
С уважением,

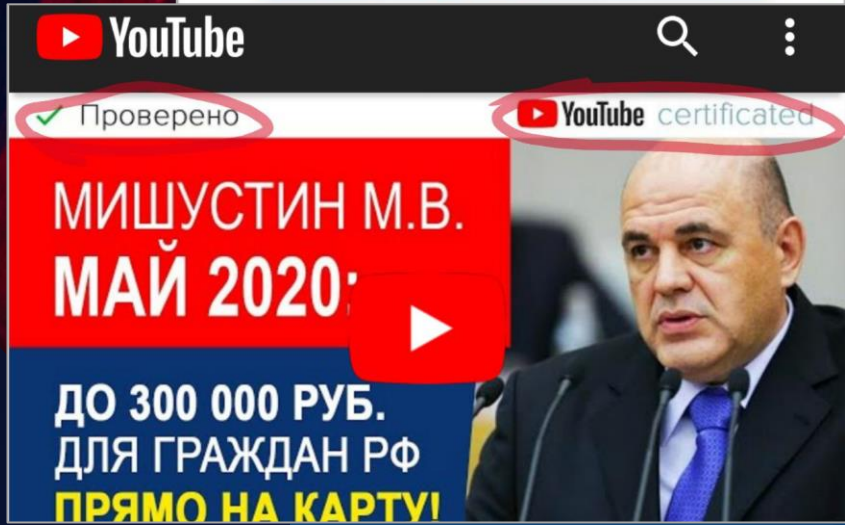
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

kaspersky

COVID19 как наживка для фишинга

- Фальшивые циркуляры/приказы
- Фальшивые компенсации
- Мошенничество под видом штрафов
- Все типы мошенничеств через SMS и IM
- Поддельные предложения дефицитных товаров
- Поддельные компенсации гражданам за отмененные мероприятия
- Массовое/целевое вымогательство



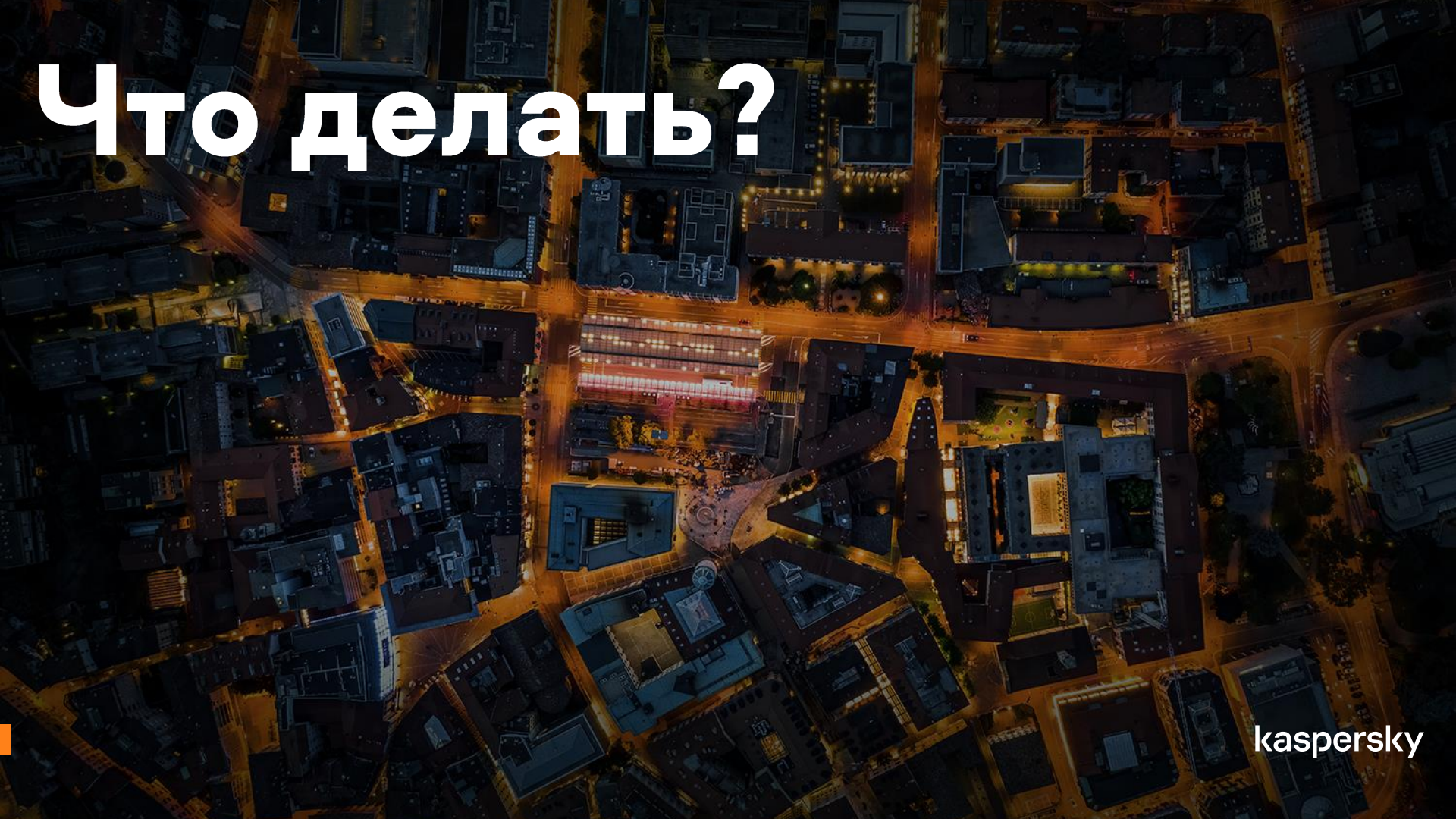


kaspersky

Главные тренды 2021

- **Атаки вымогателей на социально значимые объекты**
- **Атаки на цепочку поставок**
- **Эксплуатация уязвимостей нулевого дня**
  (примеры - Microsoft Exchange и группа Hafnium, 4 0day уязвимости в Chrome и Windows – использовались в сложной угрозе PuzzleMaker)

Что делать?



kaspersky

Простые методы защиты более не работают

ENDPOINT SECURITY
РЕШАЛА ВСЕ ПРОБЛЕМЫ

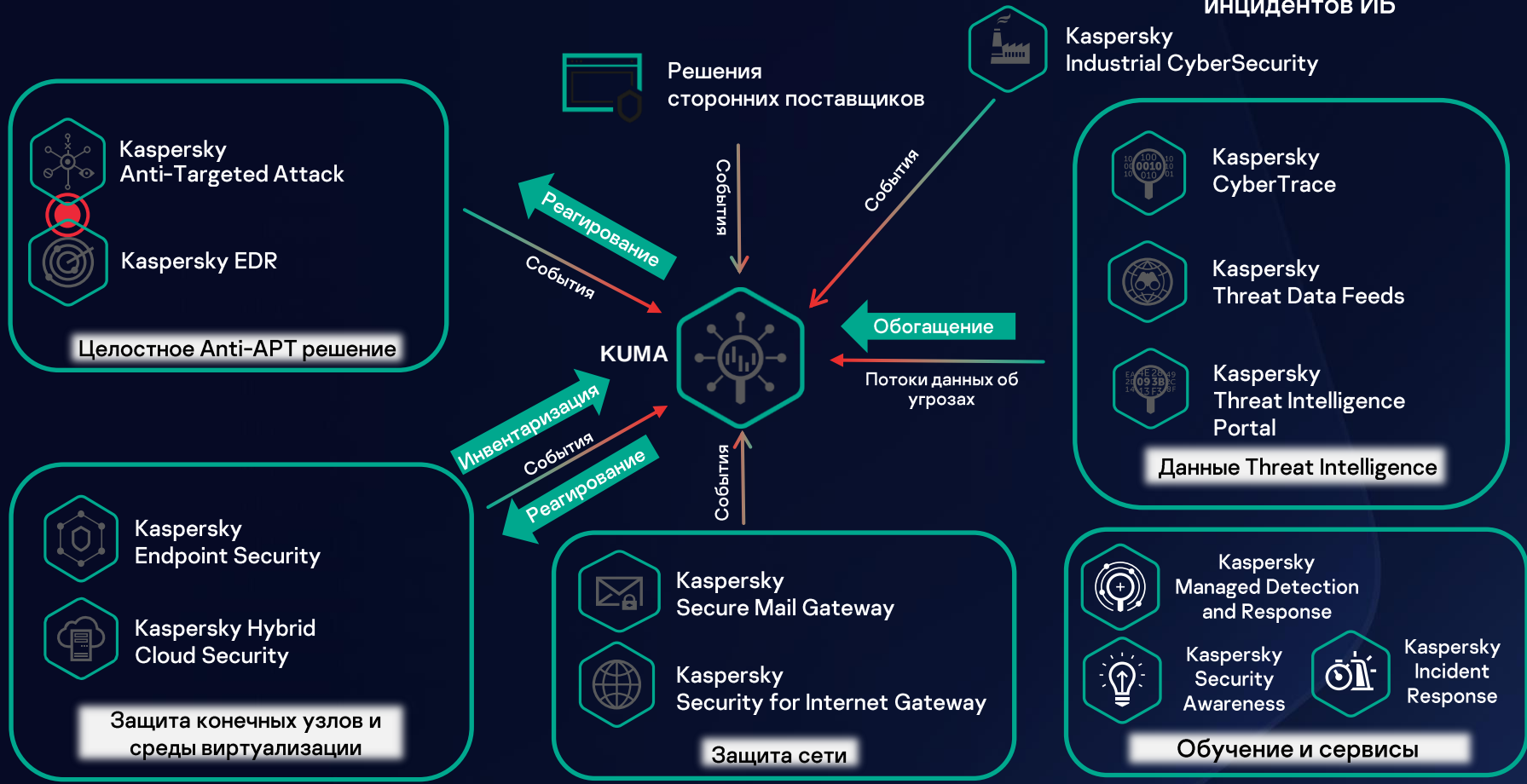
2006

2021

kaspersky

Мониторинг и реагирование на инциденты

Единая консоль мониторинга и анализа инцидентов ИБ



СПАСИБО

В 2020 эксперты Лаборатории Касперского

- Приняли участие в расследовании 300+ инцидентов
- Выпустили 121 отчёт о целевых атаках (APT)
- Отслеживали деятельность 200+ APT-групп
- Обнаруживали 360 000 новых вредоносных объектов ежедневно

kaspersky