Kaspersky
Security Day
2021

Современные угрозы и методы защиты корпоративной инфраструктуры

Булат Сираев,
Deputy Head of Global Enterprise Sales

kaspersky

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, VPNы, (виртуальные) устройства

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 APT (высокоуровневых угроз) в 2020

Top 10 targets:

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

Top 12 targeted countries and territories:

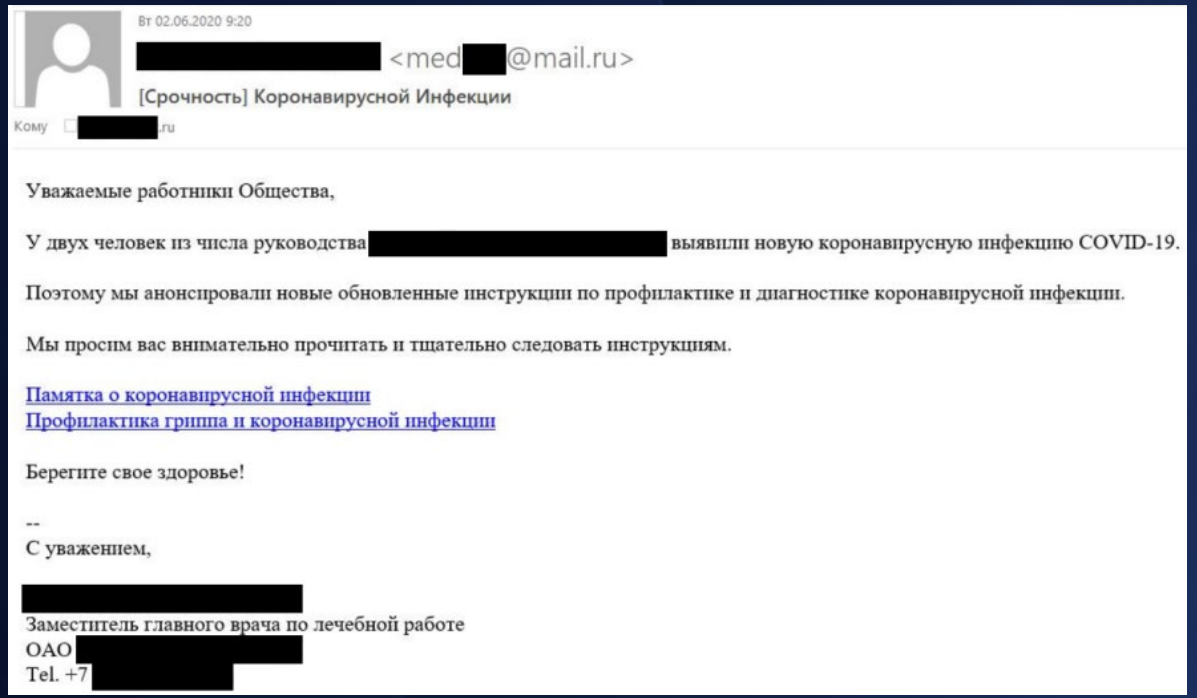
Top 10 significant threat actors:

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**



kaspersky

Lazarus

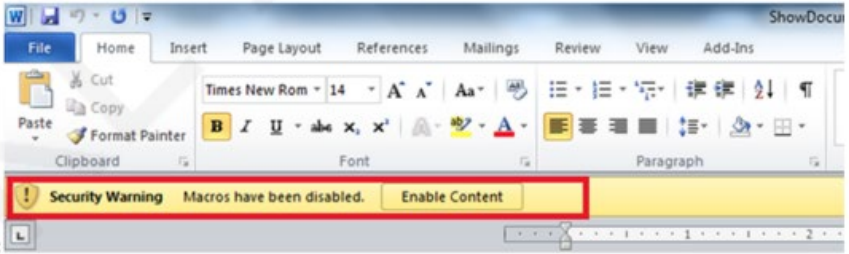
Чт 21.05.2020 12:22

[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,

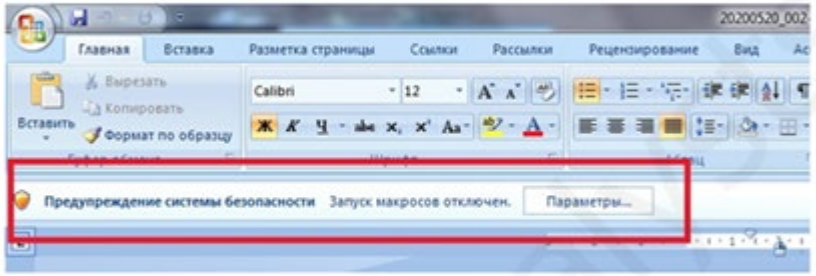
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

Чт 21.05.2020 12:36

[redacted]mail.ru>

Re[2]: Коронавирусной Инфекции

Кому [redacted]ru



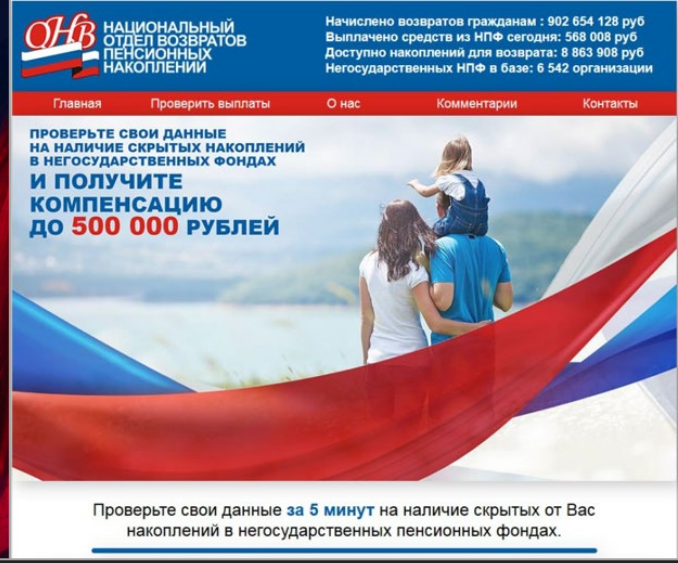
--
С уважением,

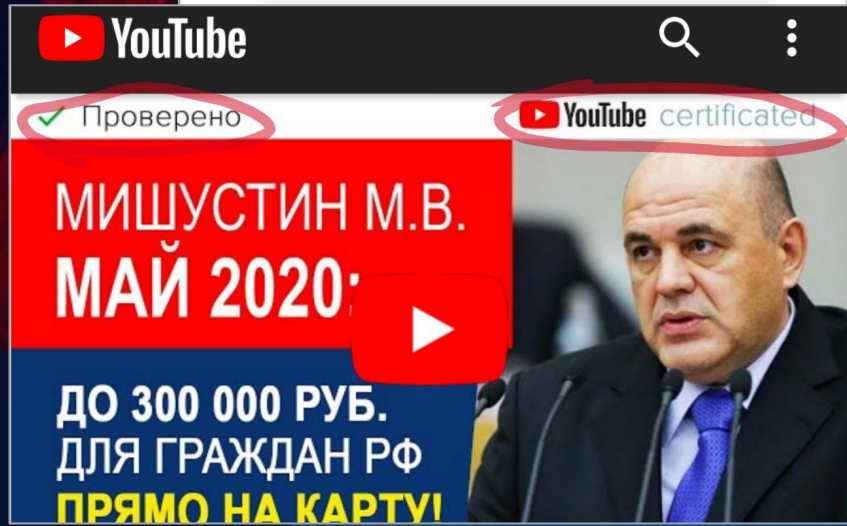
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

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 события Q1 –Q2 2021

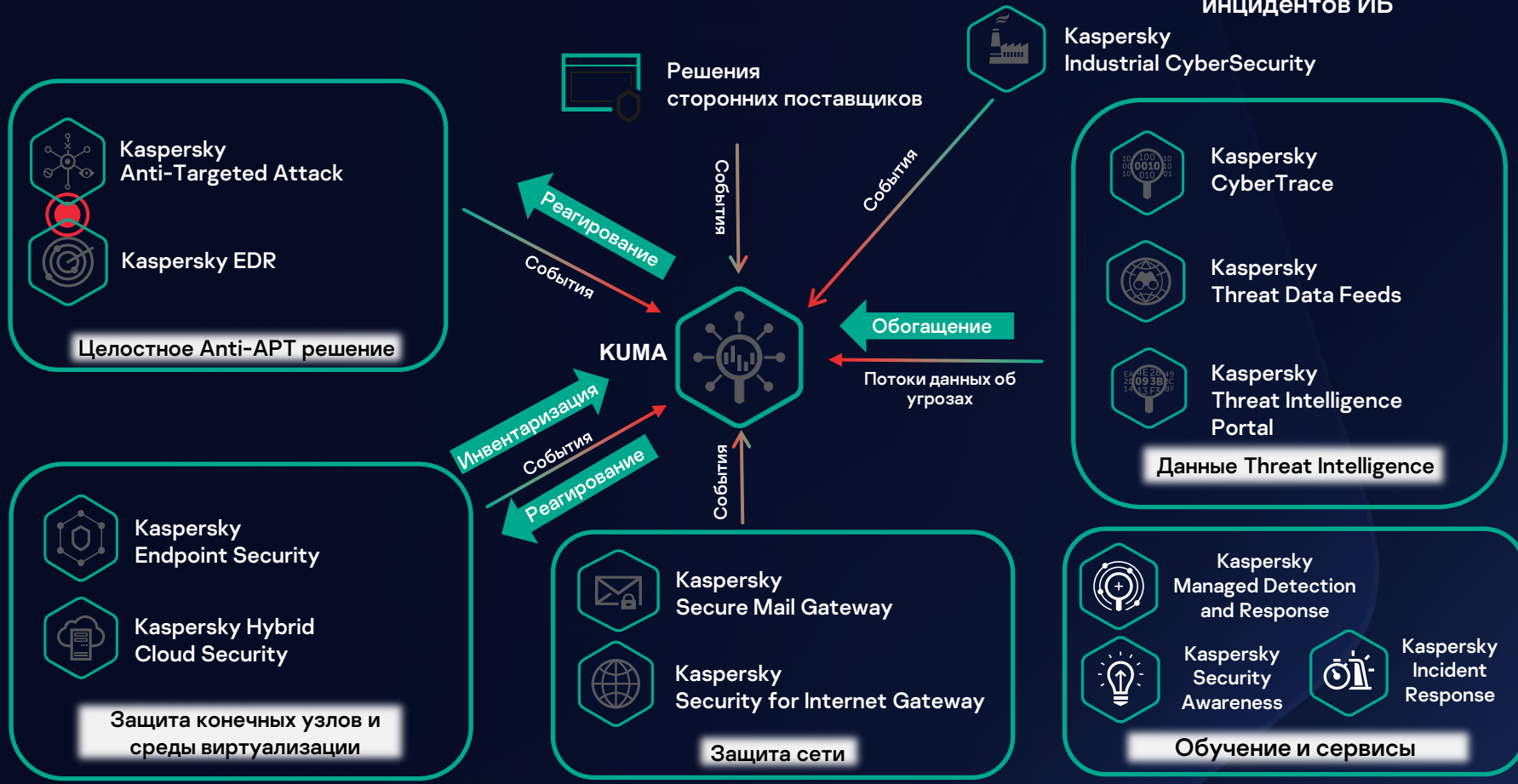
- Атаки на цепочку поставок
- Эксплуатация уязвимостей нулевого дня Microsoft Exchange
- Обнаружение Лабораторией Касперского блока из 4х уязвимостей 0-дня в Chrome и Windows, используемых в APT PuzzleMaker
- Атаки вымогателей на социально значимые объекты

Что делать?

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