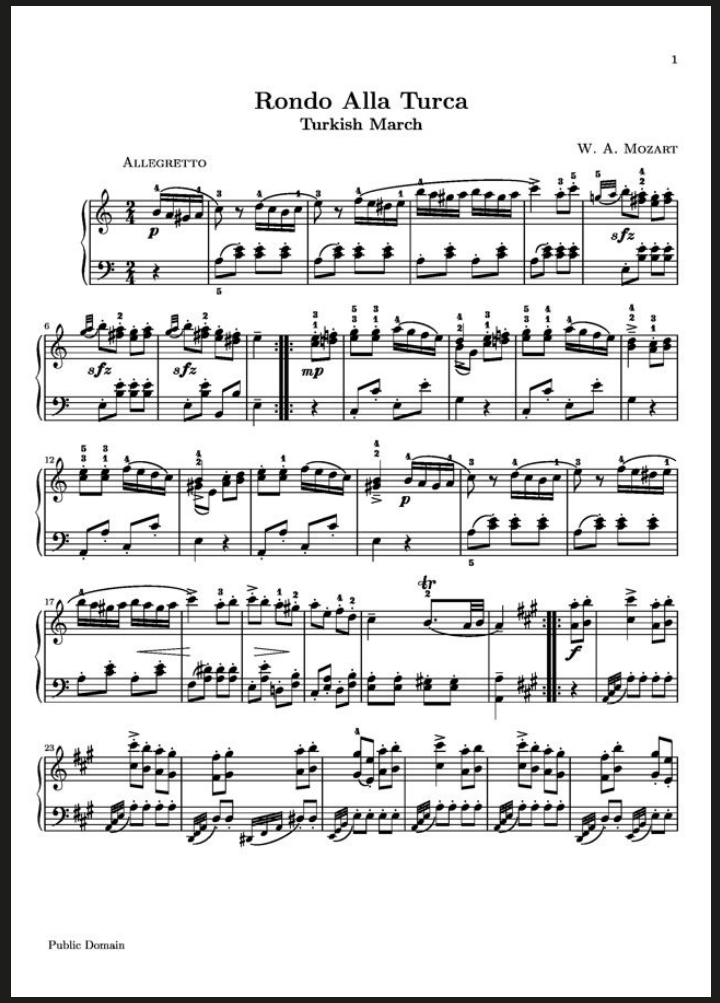
KSD 2022
Kaspersky Security Day

Актуальные тенденции кибербезопасности и современный ландшафт угроз

Дмитрий Галов
Эксперт по кибербезопасности

kaspersky 25 лет

whoami



1

Rondo Alla Turca

Turkish March

W. A. Mozart

Allegretto

Public Domain

Ожидания

Реальность

GREAT
GLOBAL RESEARCH & ANALYSIS TEAM

Marco Preuss
Director of GReAT Europe
GReAT Europe

Christian Funk
Head of GReAT, Germany
GReAT Europe

David Emm
Principal Security Researcher
GReAT Europe

Sergey Lozhkin
Lead Security Researcher
GReAT Europe

Lee Munson
Senior Technical Editor
GReAT Europe

Dani Creus
Lead Security Researcher
GReAT Europe

Marc Rivero
Senior Security Researcher
GReAT Europe

Jornt van der Wiel
Senior Security Researcher
GReAT Europe

Ivan Kwiatkowski
Senior Security Researcher
GReAT Europe

Pierre Delcher
Senior Security Researcher
GReAT Europe

Mark Lechtik
Senior Security Researcher
GReAT Europe

Ariel Jungheit
Senior Security Researcher
GReAT Europe

Giampaolo Dedola
Senior Security Researcher
GReAT Europe

Aseel Kayal
Security Researcher
GReAT Europe

Costin Raiu
Director
GReAT

Dan Demeter
Senior Security Researcher
GReAT EEMEA

Kurt Baumgartner
Principal Security Researcher
GReAT US

Dmitry Bestuzhev
Director of GReAT LatAm
GReAT LatAm

Fabio Assolini
Senior Security Researcher
GReAT LatAm

Fabio Marenghi
Senior Security Researcher
GReAT LatAm

Santiago Pontiroli
Security Researcher
GReAT LatAm

APAC

Europe

Eastern Europe

Middle East & Africa

North America

Russia

LatAm

Vitaly Kamluk
Director of GReAT APAC
GReAT APAC

Seongsu Park
Senior Security Researcher
GReAT APAC

Noushin Shabab
Senior Security Researcher
GReAT APAC

Saurabh Sharma
Senior Security Researcher
GReAT APAC

Suguru Ishimaru
Senior Security Researcher
GReAT APAC

Seth Jin
Senior Security Researcher
GReAT APAC

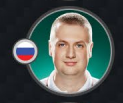
Mohamad Amin Hasbini
Director of GReAT META
GReAT META

Maher Yamout
Senior Security Researcher
GReAT META

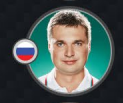
Abdessabour Arous
Security Researcher
GReAT META

Sergey Novikov
Deputy Director
GReAT

Maria Namestnikova
Head of Research Center
GReAT Russia



Igor Kuznetsov
Chief Security Researcher
GReAT Russia

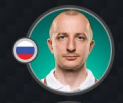


Sergey Mineev
Principal Security Researcher
GReAT Russia

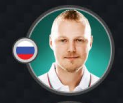
Sergey Belov
Principal Security Researcher
GReAT Russia

Victor Chebyshev
Lead Security Researcher
GReAT Russia

Boris Larin
Lead Security Researcher
GReAT Russia



Denis Legezo
Lead Security Researcher
GReAT Russia



Konstantin Zykov
Senior Research Developer
GReAT Russia

Dmitry Galov
Senior Security Researcher
GReAT Russia

Ilya Saveliev
Security Researcher
GReAT Russia

Leonid Bezvershenko
Junior Security Researcher
GReAT Russia

Georgy Kucherin
Intern
GReAT Russia

#Reverse Engineering #Security Intelligence #Digital Forensics #Mobile Security #User Security Education
#Underground Network Monitoring #Counteracting Cyber-Espionage #Internet of Things Research #Online Banking Security

kaspersky

Источники аналитических данных об угрозах

- Kaspersky Security Network
- Поисковые роботы
- Мониторинг ботнет-угроз
- Ловушки для спама
- Сенсоры
- APT-команда
- Партнеры
- Открытые источники (OSINT)

GREAT

Kaspersky APT Research team

Kaspersky SOC

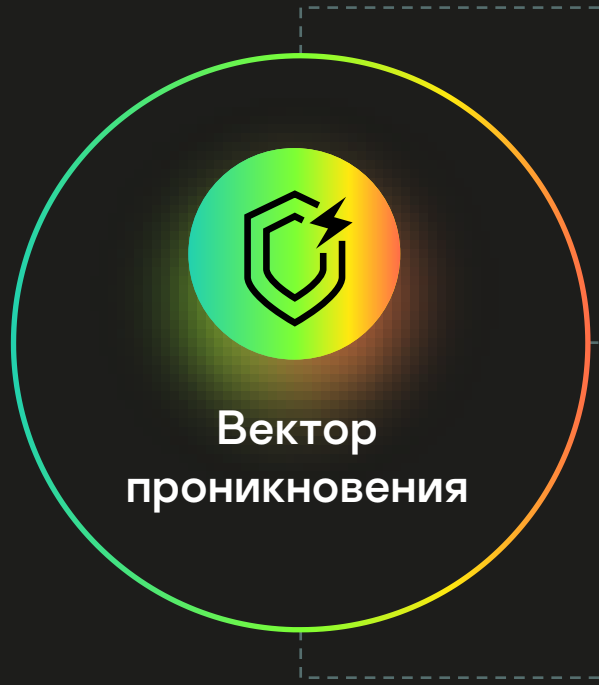
Kaspersky Red Team

Kaspersky ICS CERT

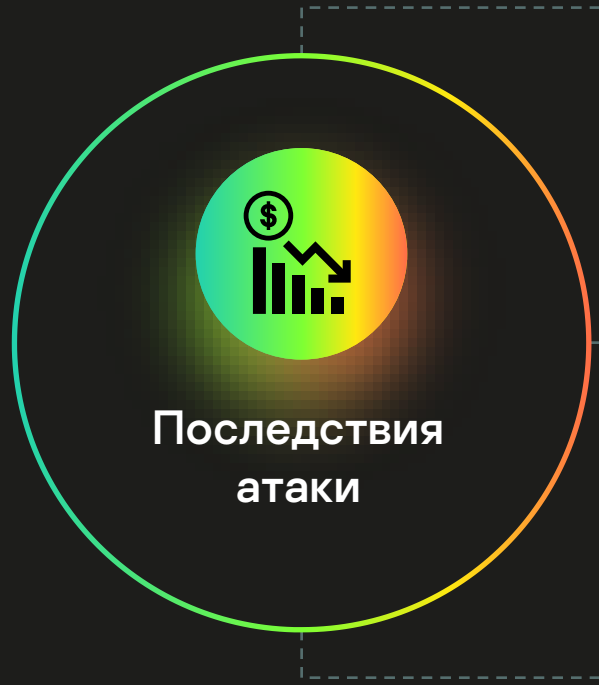
Kaspersky Threat Intelligence

Клиент

Атаки на организации в 2021 году



- 53,6% — Эксплуатация уязвимостей на периметре сети
- 17,9% — Скомпрометированные учетные данные
- 14,3% — Атаки через электронную почту



- 51,9% — Зашифрованные данные
- 16,0% — Утечка данных
- 11,1% — Компрометация Active Directory

Индустрии

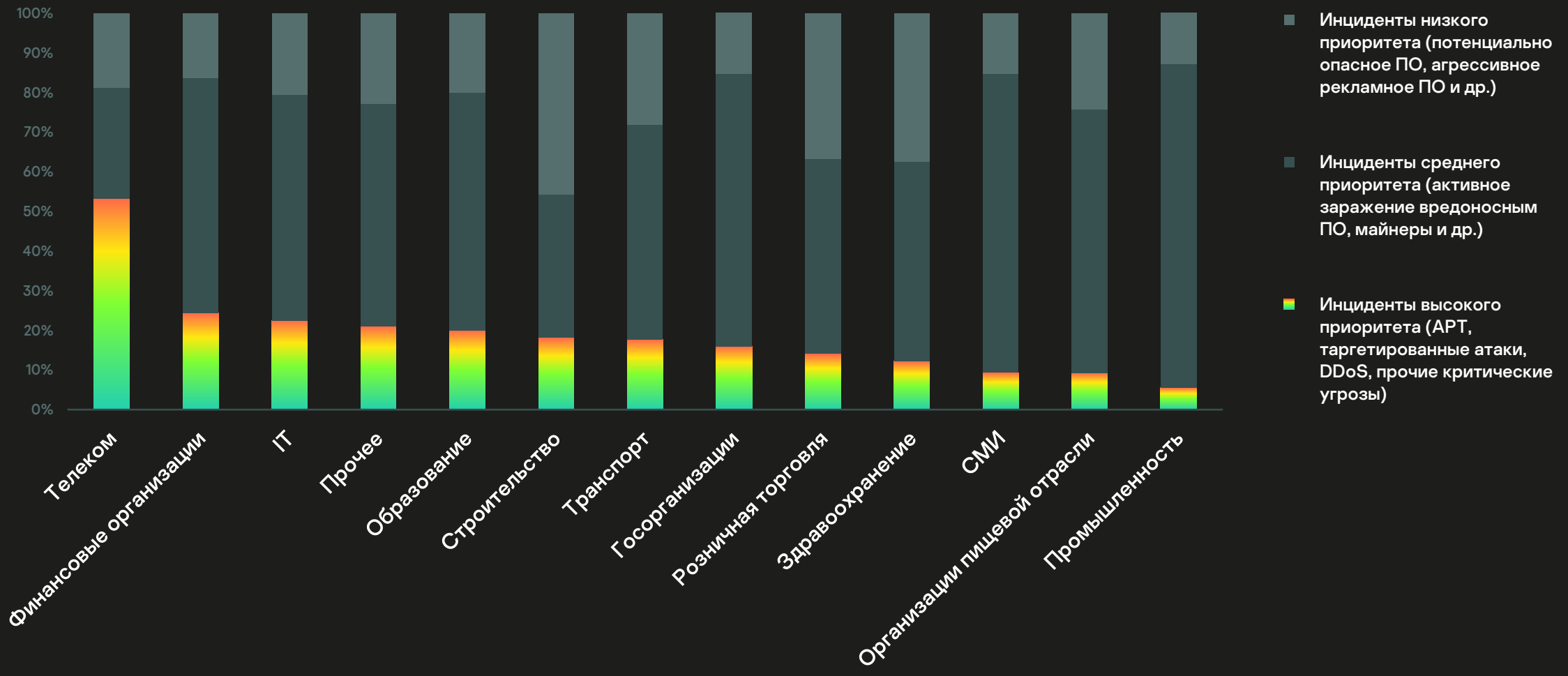
- 30,11% — Промышленные предприятия
- 19,35% — Государственный сектор
- 12,9% — Финансовые организации
- 11,83% — IT

Регионы

- 30,11% — Европа
- 30,11% — Ближний Восток и Африка
- 24,73% — СНГ
- 11,83% — Америки

Источник: Global Emergency Response Team, Kaspersky

Современные кибервызовы – статистика по отраслям экономики



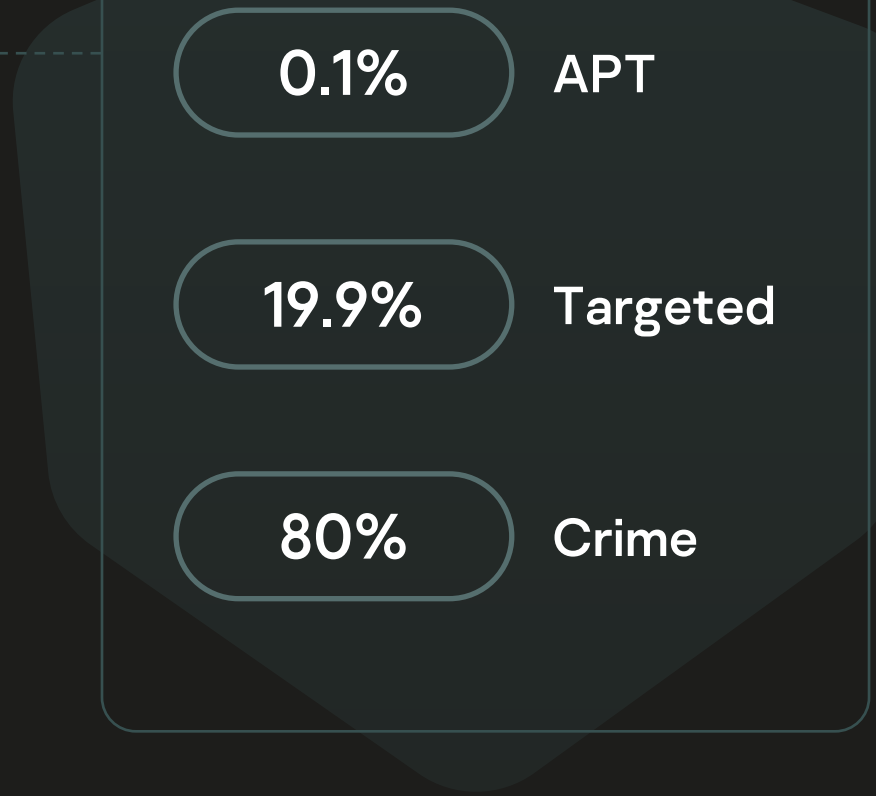
Источник данных – сервис Kaspersky Managed Detection and Response, 2021 год

Современные кибервызовы

Средний ущерб от успешной кибератаки

SMB: 105k$ **Enterprise:** ~1M$

- Эксплуатация тематики COVID-19 в 2021 году
- Атаки на удаленный доступ
- «Кроме Windows»: Linux, Mac, роутеры
- Мобильные импланты, 0day's: iOS/Android-атаки
- Атаки на цепочки поставок
- Современные шифровальщики: Ransomware-as-a-Service, Big Game Hunting
- 49.7% попыток эксплуатации уязвимостей в 2021 году приходилось на долю Microsoft Office



Источники данных: Cybersecurity Ventures, Kaspersky

Масштаб современных кибератак

1

Средний ущерб от успешной кибератаки

SMB: 105k$
Enterprise: ~1M$

2

Отношение лидеров бизнеса

68% лидеров бизнеса считают, что риски, связанные с кибербезопасностью, растут

3

Мотивация атак

71% атак были финансово мотивированными

4

Оценка активности шифровальщиков

За Q1 2022 мы защитили более 74 тыс. уникальных пользователей от шифровальщиков

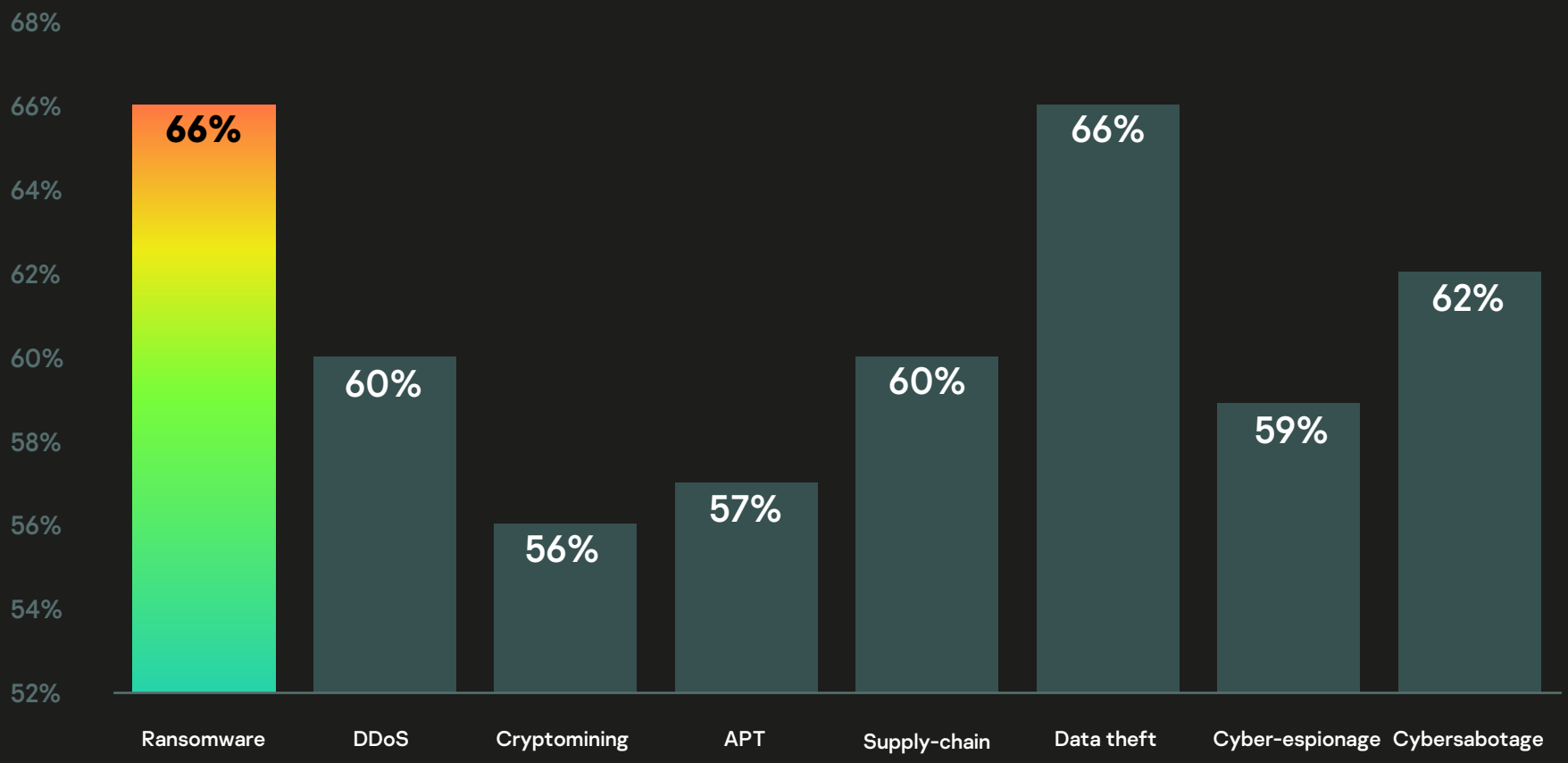
5

Особенности атак

52% атак имели отношение к взлому, 28% были проведены с использованием вредоносов, 33% использовали фишинг и социальную инженерию

Источники данных: Kaspersky, Accenture, Verizon

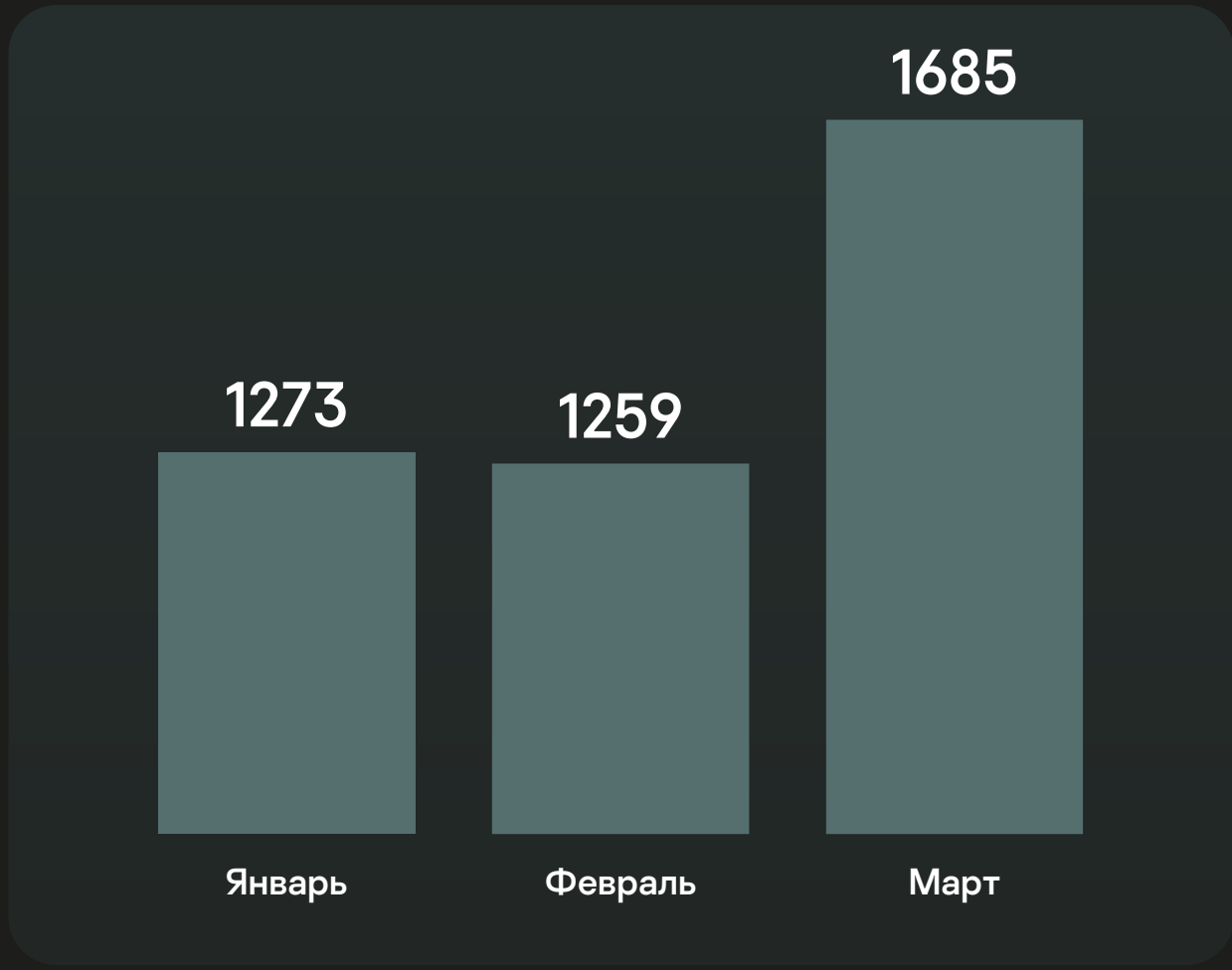
Опрос: Вероятность различных типов угроз



Источник: Kaspersky Survey, 2022

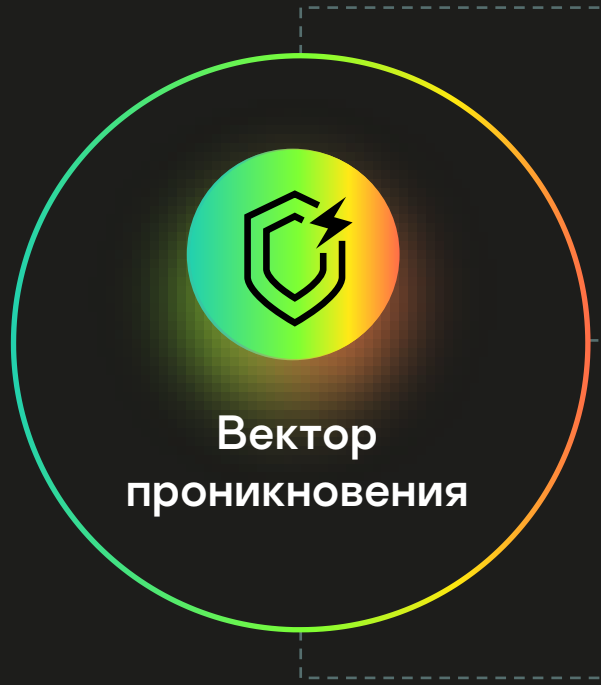
Рост атак шифровальщиков в России в марте 2022 года

Число бизнес-пользователей в РФ, столкнувшихся с шифровальщиками в 2022 году



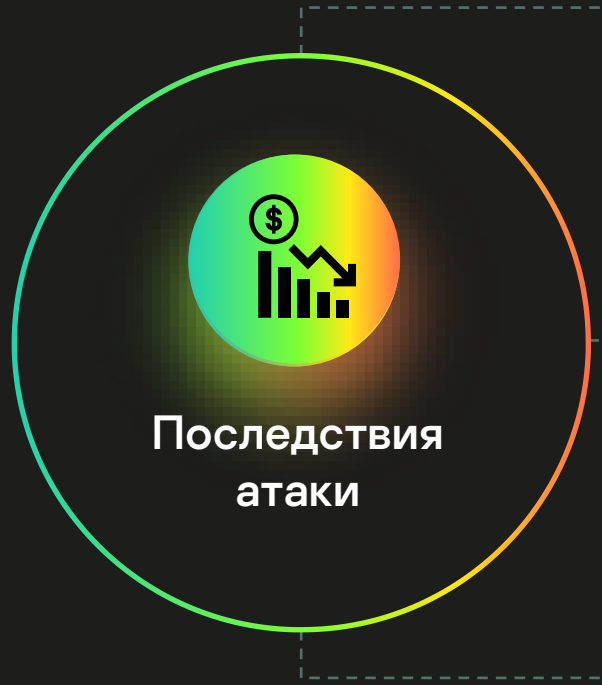
Источник: Kaspersky

Общая информация по шифровальщикам в 2021 г



Вектор проникновения

- **31,6%** — Атаки с перебором паролей (bruteforce)
- **31,5%** — Эксплуатация уязвимостей на периметре сети
- **23,7%** — Атаки через электронную почту



Последствия атаки

- **37,9%** — Зашифрованные данные
- **14,7%** — Утечка данных
- **10,5%** — Закрепление в сети с целью дальнейших злонамеренных действий

Индустрии

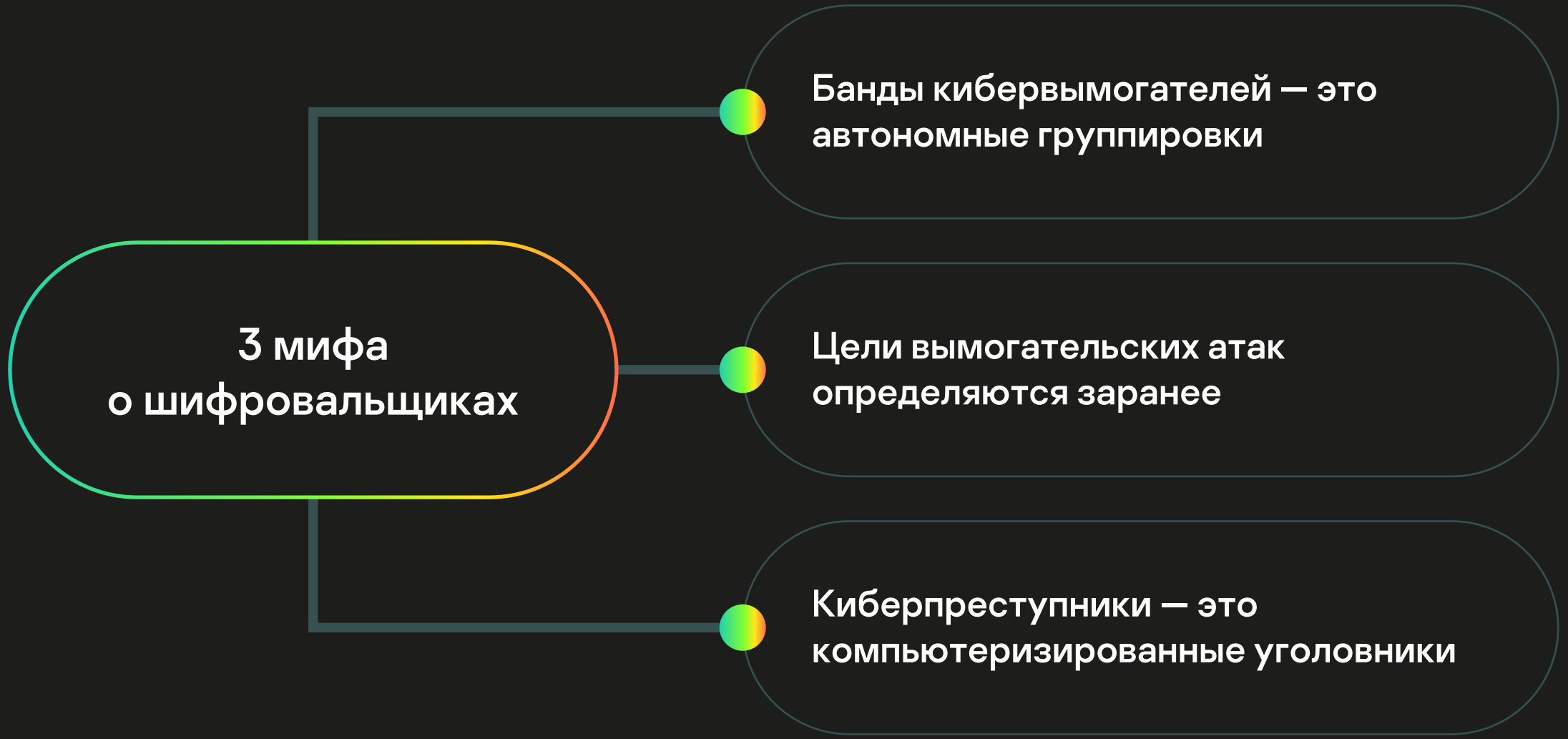
- **22%** Промышленные предприятия
- **19%** Государственный сектор
- **13%** Финансовые организации
- **13%** Телекоммуникации

Регионы

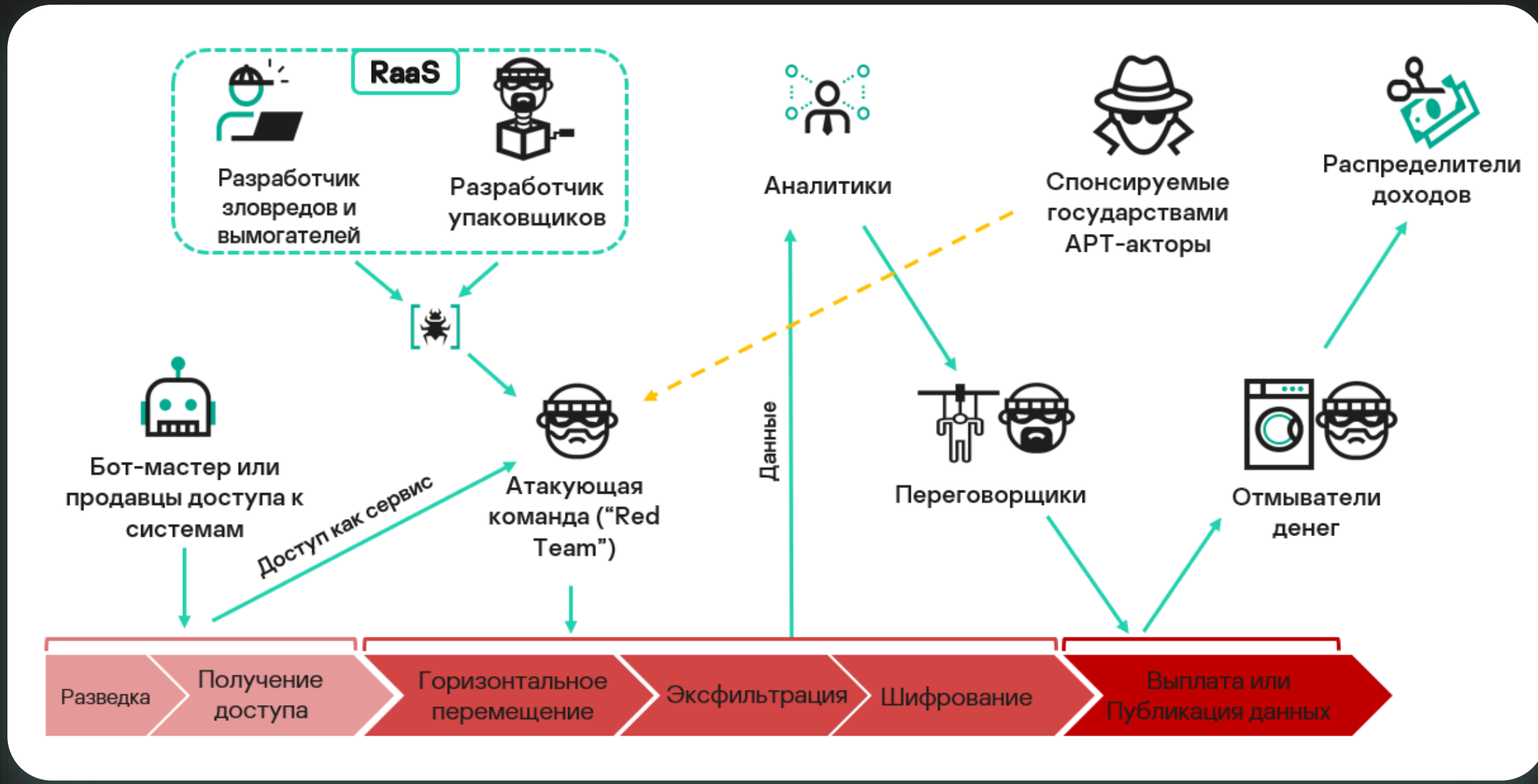
- **27,8%** СНГ
- **26,8%** Ближний Восток и Африка
- **24,7%** Европа
- **16,5%** Америки

Источник: Incident Response Analyst Report 2021, Kaspersky

Популярные мифы о шифровальщиках



Экосистема вымогательского «бизнеса»



Как противодействовать современной ransomware атаке

Критические контрмеры

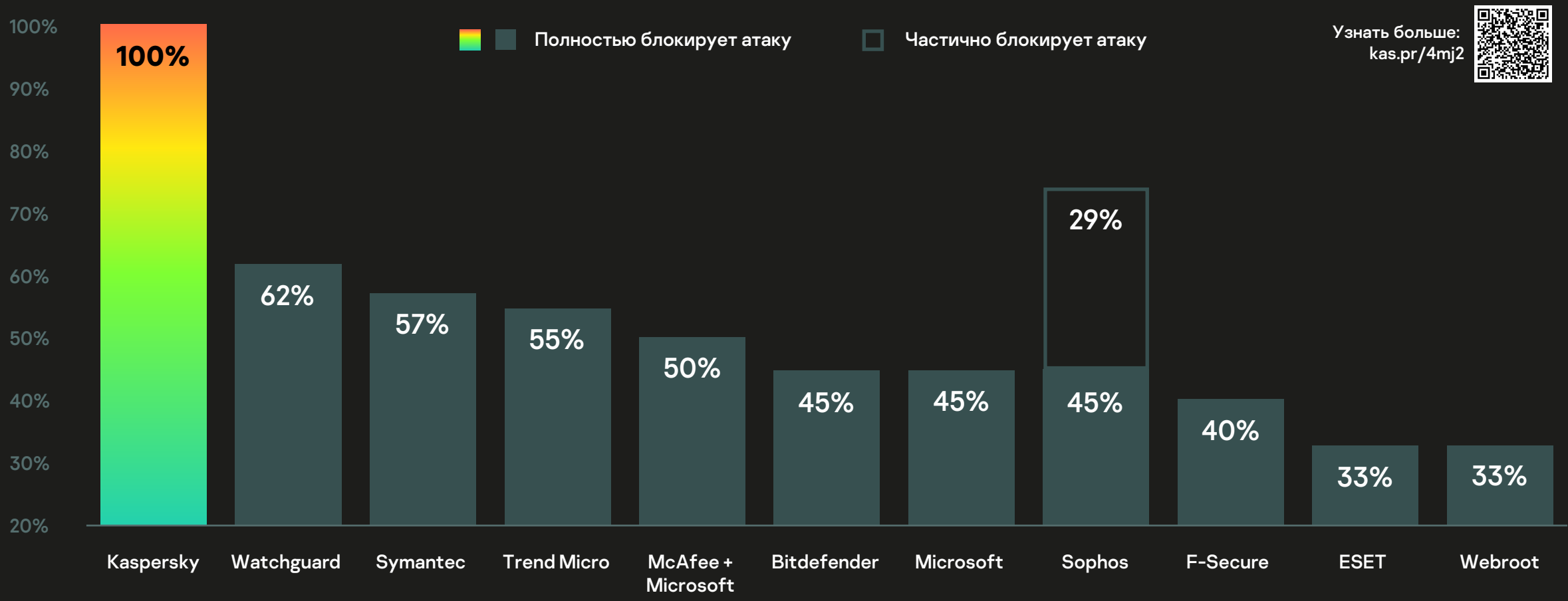
CERT NZ Critical Controls for your business

- Сервисы доступные в Интернет
- Установка обновлений
- Многофакторная аутентификация
- Сегментация сетей
- Минимальные права
- Резервирование
- Контроль запуска приложений
- Регистрация событий и алерты
- Отключение макросов
- Управление паролями

No More Ransom! Не плати!

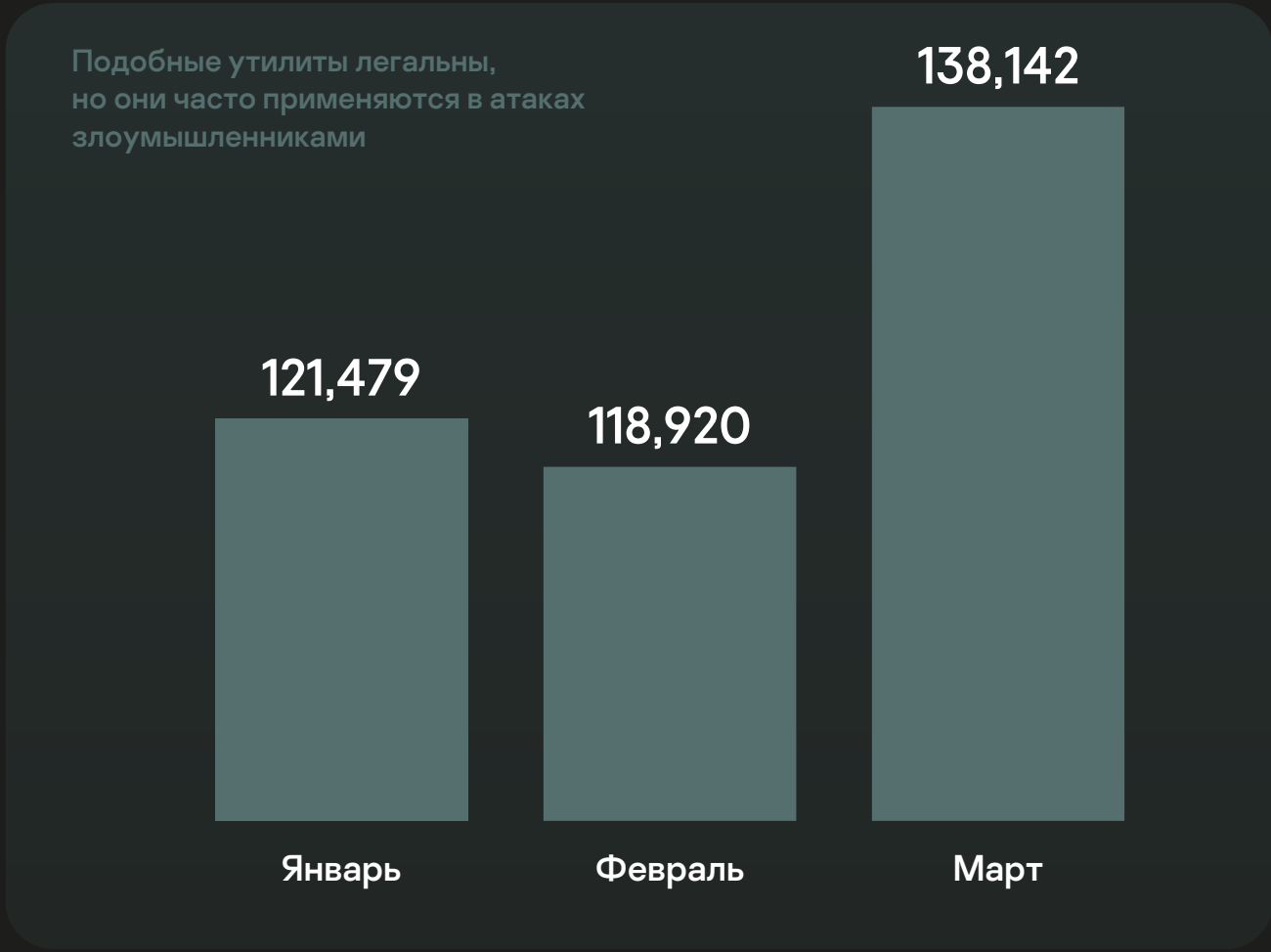
Иногда зараженному пользователю можно помочь получить доступ к зашифрованным файлам или заблокированной системе без необходимости платить выкуп. Мы создали хранилище ключей и утилит, позволяющих расшифровать данные, заблокированные троянцами-вымогателями разных типов.

Лучшая защита от шифровальщиков



Рост числа обнаружения утилит удаленного администрирования (RAT)

Число бизнес-пользователей в РФ, у которых были обнаружены утилиты удаленного администрирования в 2022 году



Источник: Kaspersky

Не только шифровальщики. MoonBounce – скрытая угроза в UEFI

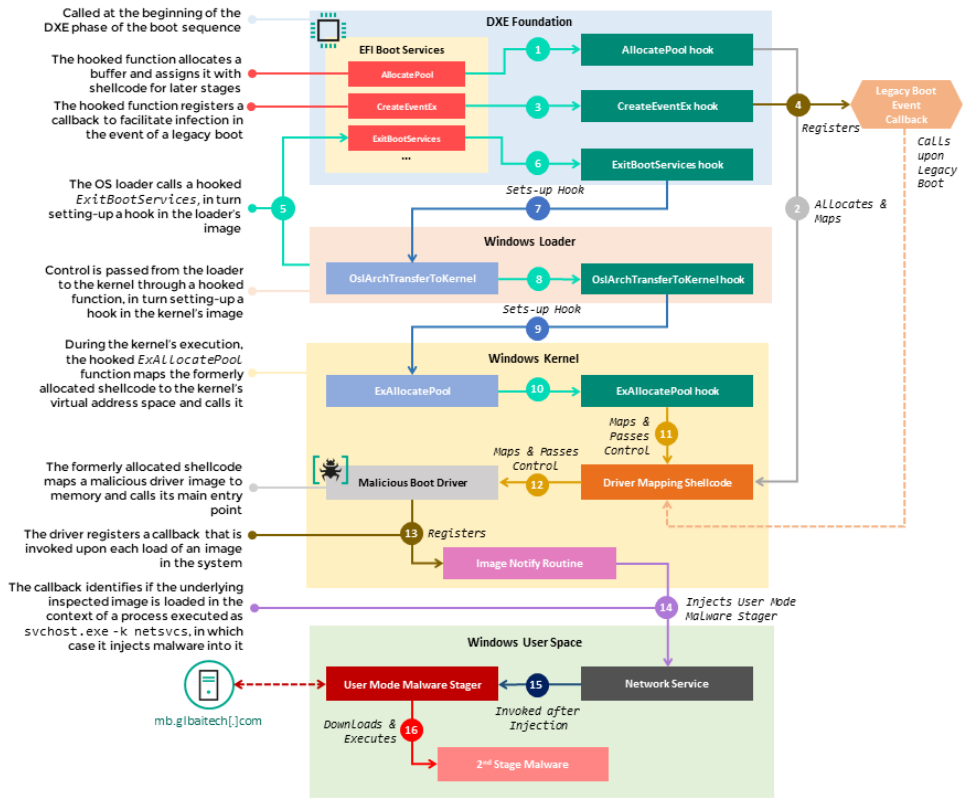


Схема загрузки и развертывания зловреда

Третий обнаруженный UEFI буткит (после LoJax и MosaicRegressor)

Имплант предназначен для развертывания бэкдора в системе пользователя

Все компоненты существуют только в оперативной памяти, никаких следов на жестких дисках не остается

Что изменилось в этом году

Рост числа кибератак в первом квартале 2022 года

Всплеск активности

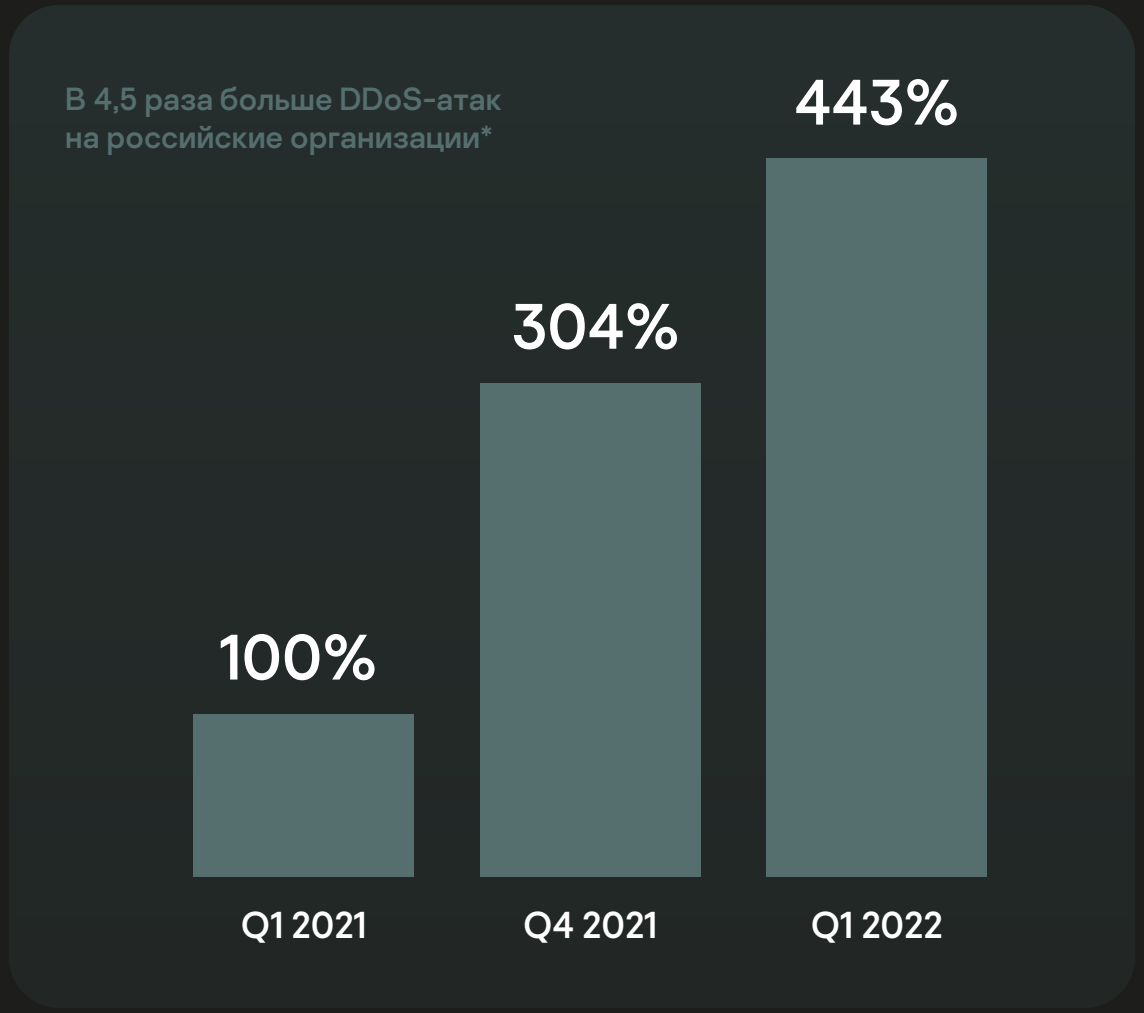
- Собственная активность «хактивистов»
- Атаки, спонсируемые иными странами
- Атаки спецслужб иных стран

Приоритеты атакующих

- Нарушение критических процессов, с максимальным уроном
- Кибершпионаж
- Пропагандистские акции и дезинформация

Мишени атакующих

- Критические инфраструктуры и важные коммерческие поставщики
- Информационные порталы и ресурсы госслужб
- Расширенный спектр компаний-целей, участвующих в важных цепочках поставок



* В Q1 2022 по сравнению с Q1 2021, по данным сервиса Kaspersky DDoS Protection

Примеры атак

Шифровальщики

Шифровальщики и вайперы

- Атаки на крупные организации, что раньше в основном встречалось лишь за рубежом
- Freeud: шифровальщик, выдвигает политические требования вместо финансовых
- RURansom: шифровальщик-вайпер, необратимо шифрует файлы по политическим мотивам

Взломы

Взломы «Anonymous» и других групп

- Похищение конфиденциальных данных с последующей публикацией
- Размещение пропаганды на публичных ресурсах
- Компрометация IoT-устройств (камеры, роутеры)

DCRat

Шпионская программа удаленного управления

- Доставляется с e-mail
- Варианты оформления – «Приказ ФСБ», прикрепленный файл «Федеральный Ативирус Аврора.exe»,
- Удаленное управление, загрузка и исполнение модулей, сбор информации о системе, кража информации, keylog, screenshots

Кризис доверия?

Риски от обновления ПО третьих сторон существенно возросли

В качестве «полезной нагрузки» зафиксировано добавление бэкдоров, вайперов, отмечены случаи саботажа, несанкционированного отображения политических баннеров и др.

Зафиксировано несколько десятков открытых репозиториев, в которые были внесены изменения (либо фиксировались такие попытки)

Организации опасаются устанавливать обновления ПО, ожидая возможных блокировок. Но это усиливает риски атак

Уход иностранных поставщиков решений для киберзащиты

Многие российские пользователи и организации оказались в одном из самых киберопасных регионов мира

Без защиты

Полагаться на еще работающее импортное решение опасно

Оно может быть заблокировано в любой момент

Компании лишились защиты

Иностранные продукты не обновляются или блокируются

Оставшиеся иностранные вендоры могут уйти

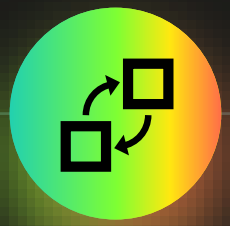
С теми же последствиями для заказчика

Комплексный подход к защите бизнеса

Ключевые элементы защиты

Квалифицированный персонал

Эффективность современных комплексных защитных решений напрямую коррелирует с уровнем экспертизы ИБ- и SOC-команд, работающих с ними. Организациям следует инвестировать в обучение сотрудников или воспользоваться услугами сторонних MDR-сервисов от надежного поставщика



Надежные защитные решения

Экспертам ИБ/SOC требуются решения, которые надежно обеспечат мониторинг всего, что происходит в сети организации с точки зрения кибербезопасности, и с максимальной степенью автоматизации помогут своевременно обнаружить и заблокировать угрозы. Решения, на которые можно положиться и в нашей новой реальности

Аналитические данные Threat Intelligence

Без актуальной и релевантной информация о том, какие злоумышленники представляют угрозу для организации, как они действуют и какими инструментами пользуются, невозможно обеспечить защиту от современных киберугроз. Использование данных Threat Intelligence должно стать неотъемлемой частью стратегии защиты

KSD 2022

Kaspersky Security Day

Спасибо!

kaspersky 25 лет