KSD 2023
Kaspersky Security Day

Место действия – 2023 год: современные угрозы и методы защиты

Дмитрий Галов

Старший исследователь угроз информационной безопасности, «Лаборатория Касперского»

kaspersky

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

Marco Preuss
Deputy Director, GReAT
GReAT Europe

Christian Funk
Head of GReAT, Germany
GReAT Europe

David Emm
Principal 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

Ariel Jungheit
Senior Security Researcher
GReAT Europe

Giampaolo Dedola
Senior Security Researcher
GReAT Europe

Robin Kwiatkowski
Security Researcher
GReAT Europe

Costin Raiu
Director
GReAT

Dan Demeter
Senior Security Researcher
GReAT EEMEA

Kurt Baumgartner
Principal Security Researcher
GReAT US

Fabio Assolini
Director of GReAT, LatAm
GReAT LatAm

Fabio Marenghi
Senior Security Researcher
GReAT LatAm

Anderson Leite
Security Researcher
GReAT LatAm

Lisandro Ubiedo
Security Researcher
GReAT LatAm

Leandro Cuozzo
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

Jin Ye
Senior Security Researcher
GReAT APAC

Mohamad Amin Hasbini
Director of GReAT META
GReAT META

Sergey Lozhkin
Lead Security Researcher
GReAT META

Maher Yamout
Senior Security Researcher
GReAT META

Abdessabour Arous
Security Researcher
GReAT META

Mert Degirmenci
Security Researcher
GReAT META

Igor Kuznetsov
Chief Security Researcher,
Head of GReAT Russia
GReAT Russia

Sergey Mineev
Principal Security Researcher
GReAT Russia

Sergey Belov
Principal Security Researcher
GReAT Russia

Boris Larin
Lead Security Researcher
GReAT Russia

Tatyana Shishkova
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
Junior Security Researcher
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

Источники аналитических данных об угрозах

403 000

Уникальных вредоносных объектов мы детектируем ежедневно (380 000 в 2021)

122 млн

Всего вредоносных файлов обнаружено за 2022 (на 6 млн больше, чем в 2021)

> 99%

Детектируются автоматизированными системами

> 200

Активных групп, связанных с Advanced Persistent Threat

80%

Массовые угрозы

19.9%

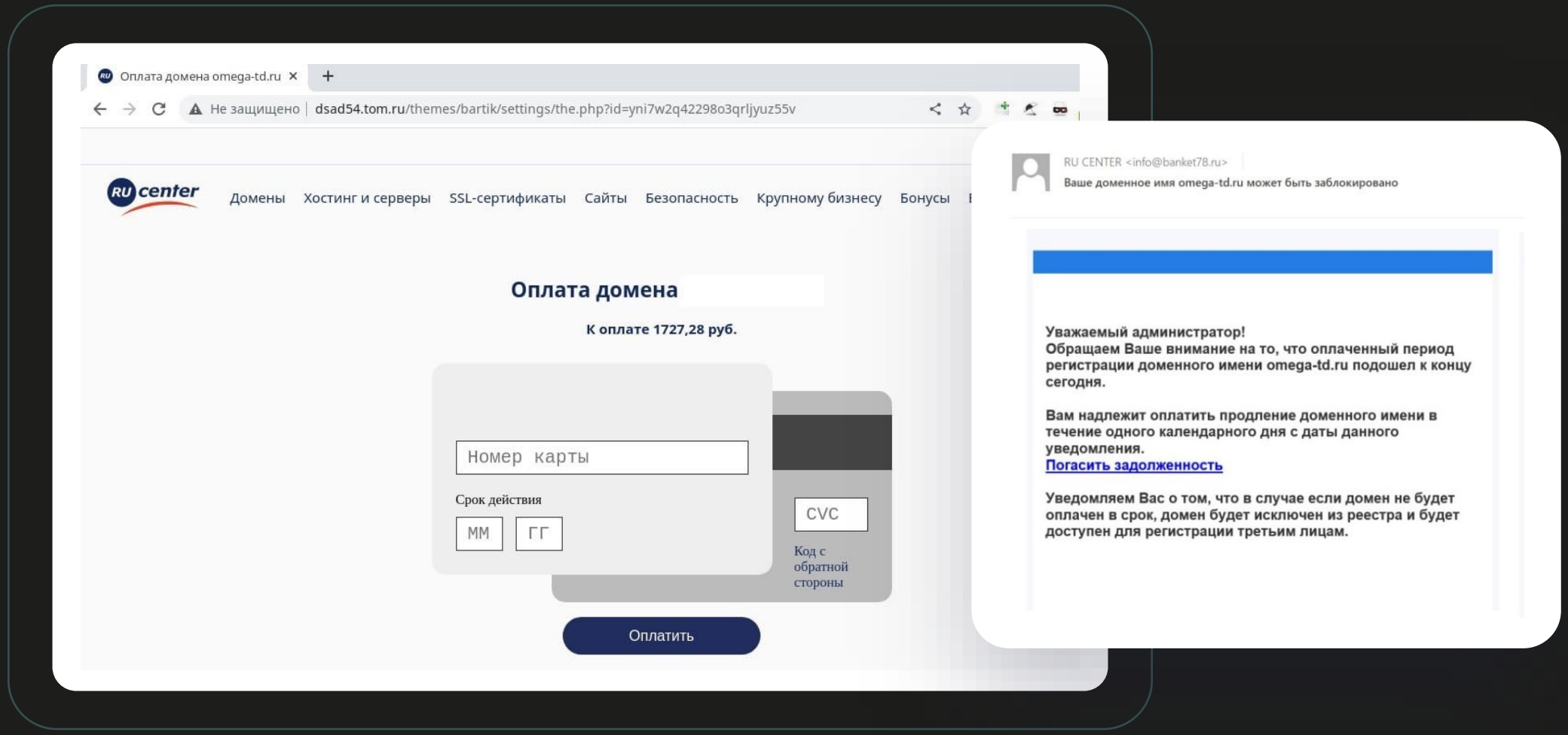
Целевые атаки

0.01%

APT

Массовые угрозы

Бизнес-скам


Оплата домена omega-td.ru
Не защищено | dsad54.tom.ru/themes/bartik/settings/the.php?id=yni7w2q42298o3qrljyuz55v
RU center
Домены
Хостинг и серверы
SSL-сертификаты
Сайты
Безопасность
Крупному бизнесу
Бонусы
Оплата домена
К оплате 1727,28 руб.
Номер карты
Срок действия
ММ
ГГ
CVC
Код с обратной стороны
Оплатить
RU CENTER <info@banket78.ru>
Ваше доменное имя omega-td.ru может быть заблокировано
Уважаемый администратор!
Обращаем Ваше внимание на то, что оплаченный период регистрации доменного имени omega-td.ru подошел к концу сегодня.
Вам надлежит оплатить продление доменного имени в течение одного календарного дня с даты данного уведомления.
Погасить задолженность
Уведомляем Вас о том, что в случае если домен не будет оплачен в срок, домен будет исключен из реестра и будет доступен для регистрации третьим лицам.

1

Атаки на службу удалённого рабочего стола (RDP)

злоумышленники используют подобранные или украденные ранее учётные данные

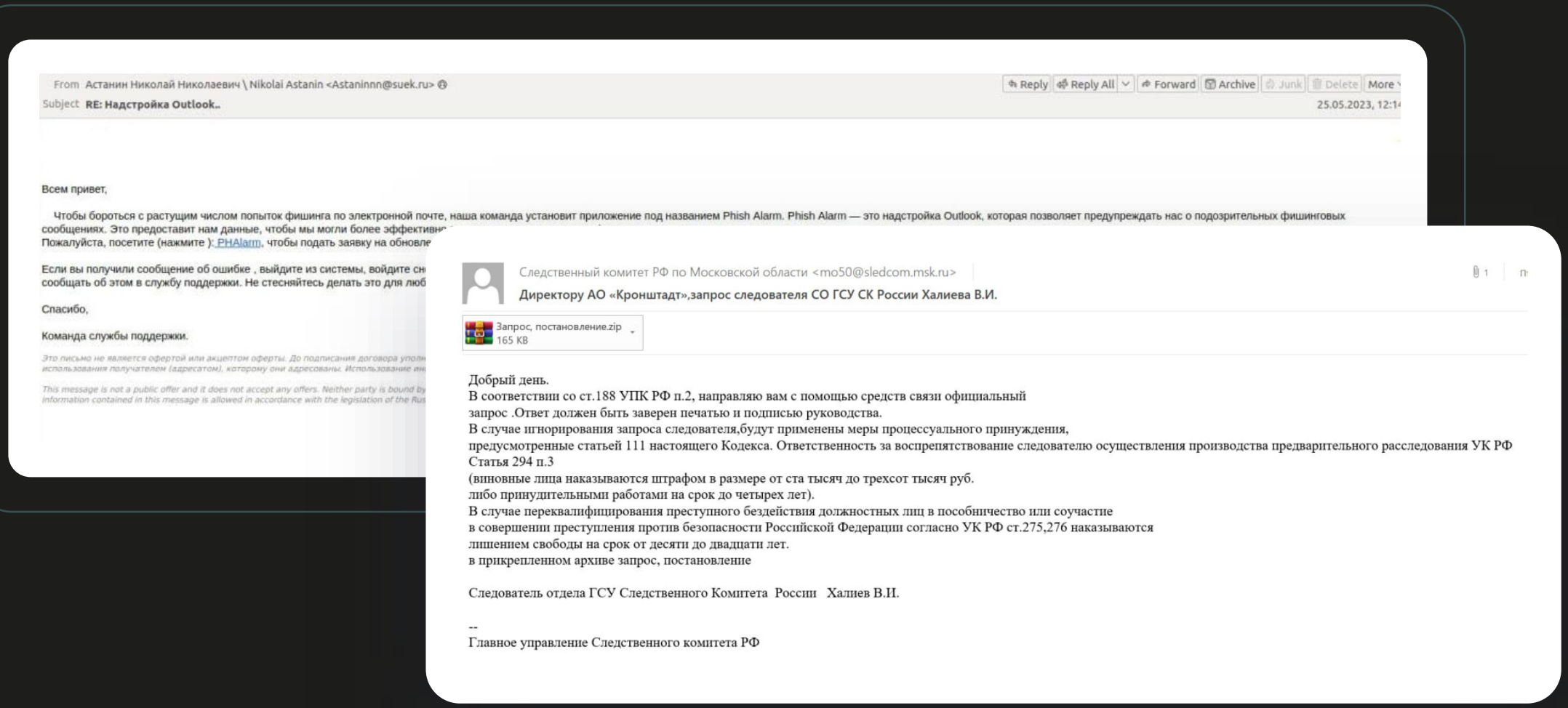
2

Фишинговые письма с вредоносными вложениями или ссылками

3

Вредоносные файл на общедоступных ресурсах под видом образцов документов

Письма



From Астанин Николай Николаевич \ Nikolai Astanin <Astaninnn@suek.ru>

Subject RE: Надстройка Outlook..

Reply | Reply All | Forward | Archive | Junk | Delete | More

25.05.2023, 12:14

Всем привет,

Чтобы бороться с растущим числом попыток фишинга по электронной почте, наша команда установит приложение под названием Phish Alarm. Phish Alarm — это надстройка Outlook, которая позволяет предупреждать нас о подозрительных фишинговых сообщениях. Это предоставит нам данные, чтобы мы могли более эффективн

Пожалуйста, посетите (нажмите): PHAlarm, чтобы подать заявку на обновле

Если вы получили сообщение об ошибке , выйдите из системы, войдите сн

сообщать об этом в службу поддержки. Не стесняйтесь делать это для люб

Спасибо,

Команда службы поддержки.

Это письмо не является офертой или акцептом оферты. До подписания договора уполн

использования получателем (адресатом), которому они адресованы. Использование ин

This message is not a public offer and it does not accept any offers. Neither party is bound by

information contained in this message is allowed in accordance with the legislation of the Rus

Следственный комитет РФ по Московской области <mo50@sledcom.msk.ru>

Директору АО «Кронштадт»,запрос следователя СО ГСУ СК России Халиева В.И.

Запрос, постановление.zip
165 KB

Добрый день.
В соответствии со ст.188 УПК РФ п.2, направляю вам с помощью средств связи официальный
запрос .Ответ должен быть заверен печатью и подписью руководства.
В случае игнорирования запроса следователя,будут применены меры процессуального принуждения,
предусмотренные статьей 111 настоящего Кодекса. Ответственность за воспрепятствование следователю осуществления производства предварительного расследования УК РФ
Статья 294 п.3
(виновные лица наказываются штрафом в размере от ста тысяч до трехсот тысяч руб.
либо принудительными работами на срок до четырех лет).
В случае переквалифицирования преступного бездействия должностных лиц в пособничество или соучастие
в совершении преступления против безопасности Российской Федерации согласно УК РФ ст.275,276 наказываются
лишением свободы на срок от десяти до двадцати лет.
в прикрепленном архиве запрос, постановление

Следователь отдела ГСУ Следственного Комитета России Халиев В.И.

--
Главное управление Следственного комитета РФ

80%

Массовые угрозы

19.9%

Целевые атаки

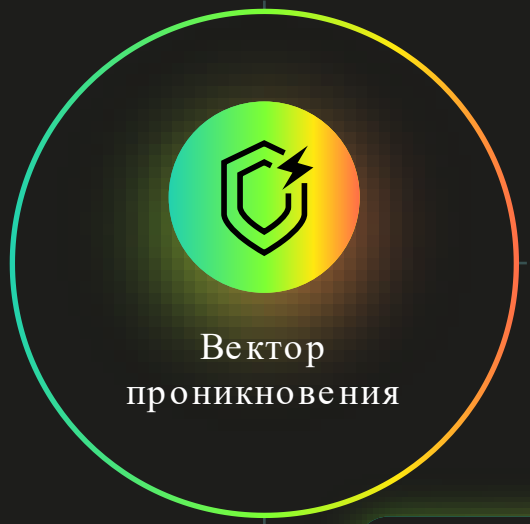
0.01%

APT

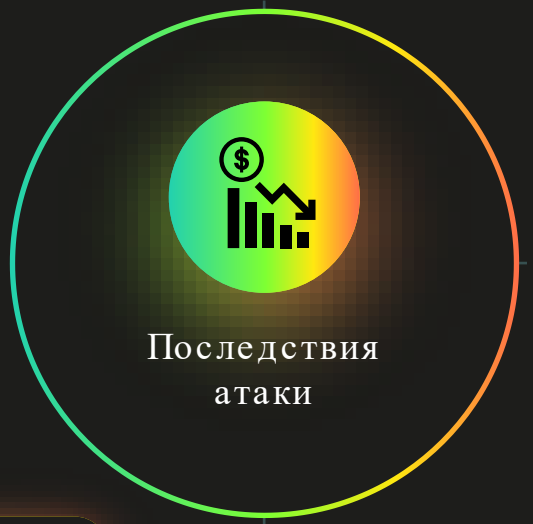
Целевые атаки

Общая информация по инцидентам в 2022 году

80,9% попыток эксплуатации уязвимостей в 3 квартале 2022 года имели отношение к Microsoft Office



- 42,9% — Эксплуатация уязвимостей на периметре сети
- 23,8% — Скомпрометированные аккаунты
- 11,9% — Атаки через почту



- 39,8% — Зашифрованные данные
- 18,4% — Утечка данных
- 17,3% — Компрометация Active Directory

В 2022 году Лаборатория Касперского заблокировала 507 млн попыток перехода по фишинговым ссылкам. 57% представителей бизнеса в России считают ключевой проблемой кибербезопасности низкий уровень цифровой грамотности сотрудников

Индустрии

19,4%	18,4%	17,4%	9,2% (+6%)
Государственный сектор	Финансовые организации	Промышленность	Телекоммуникации

Регионы

45,9%	22,5%	14,3%	13,3%
СНГ	Ближний Восток	Америка	Европа

Источник: Incident Response Analyst Report 2022, Kaspersky

Масштаб современных киберугроз для бизнеса

1

Отношение руководителей

68% руководителей считают, что ИБ-риски растут

2

Мотивация кибератак

71% атак финансово мотивированы

3

Рост атак шифровальщиков

В 2021-2022 доля пользователей, которые подверглись целевым атакам выросла почти в два раза

4

Инциденты

Уже три года шифрование данных остается для пользователей проблемой №1

5

Это плохо?

Количество попыток заражений упало на 36% в I квартале 2023 по сравнению с аналогичным периодом прошлого года

Да, но ситуация становится ещё более непростой!

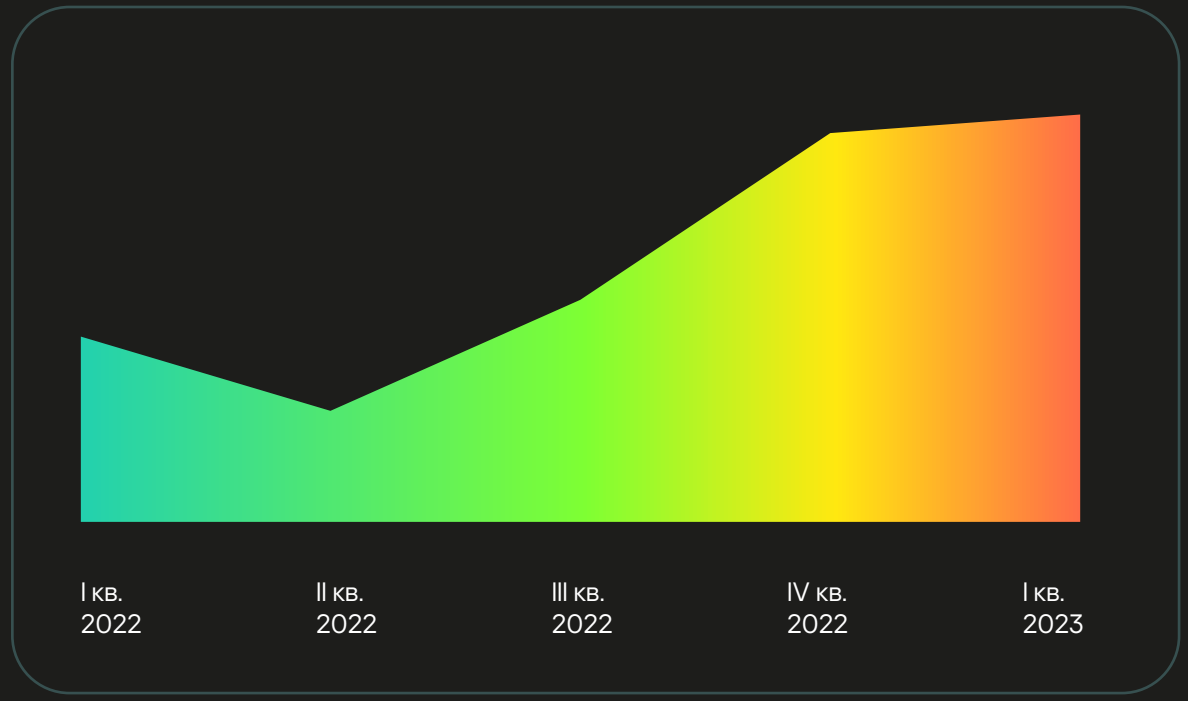
Kaspersky, Accenture, Verizon

Статистика по атакам шифровальщиков

Статистика по атакам шифровальщиков

Статистика по атакам шифровальщиков

Количество обращений в связи с успешными атаками шифровальщиков



Атакуемые отрасли

Недвижимость

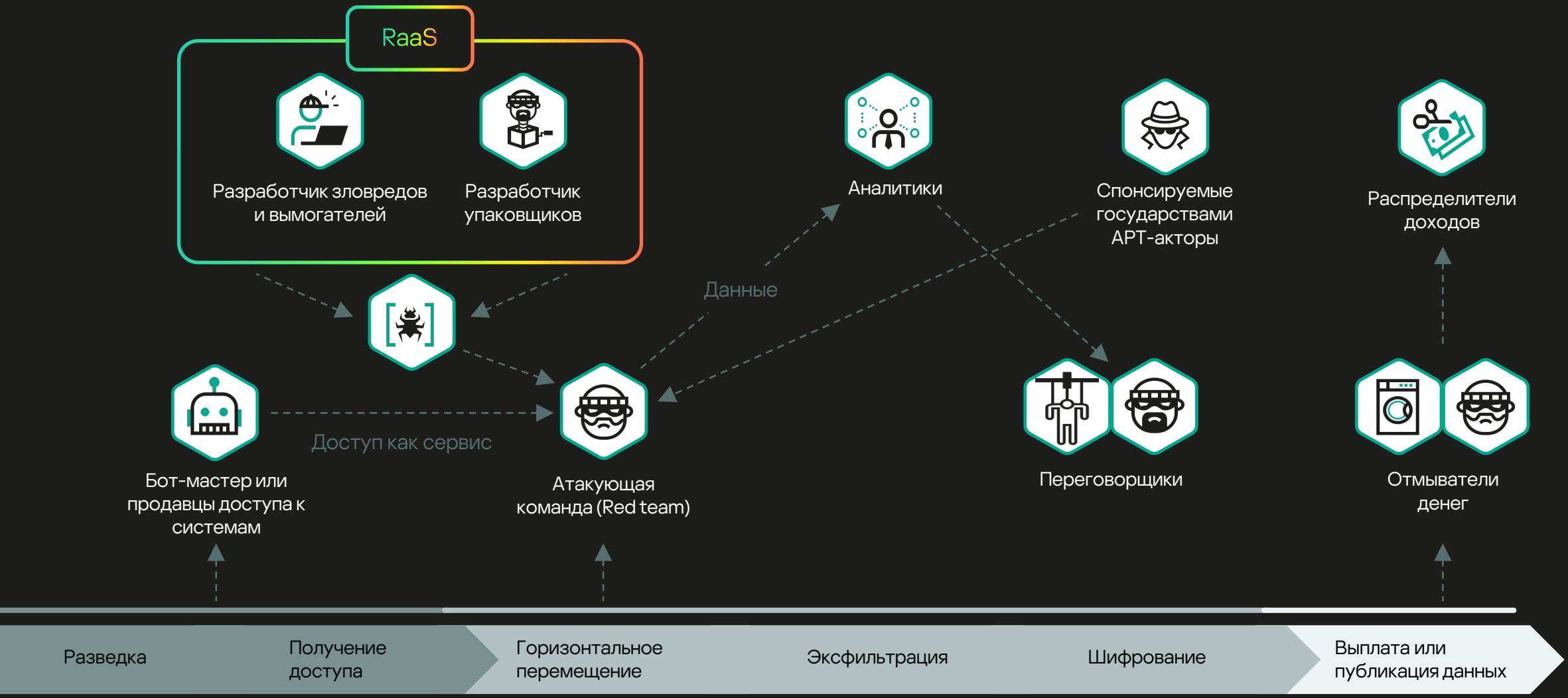
Телекоммуникационные услуги

E-commerce

Финансовые услуги

Небольшие производства

Экосистема вымогательского «бизнеса»



Новые технические возможности

Мульти-платформенные шифровальщики становятся максимально адаптивными, новые техники самозащиты

Различные «бизнес-планы»

Для привлечения большего числа аффилированных лиц. Например, Lockbit поддерживает 3 различные версии одновременно

0 days

Киберпреступники могут позволить покупку уязвимостей нулевого дня. Ранее они использовались только в APT атаках

https://securelist.com/nokoyawa-ransomware-attacks-with-windows-zero-day/109483/

Как противодействовать современной ransomware атаке

Первоначальный доступ

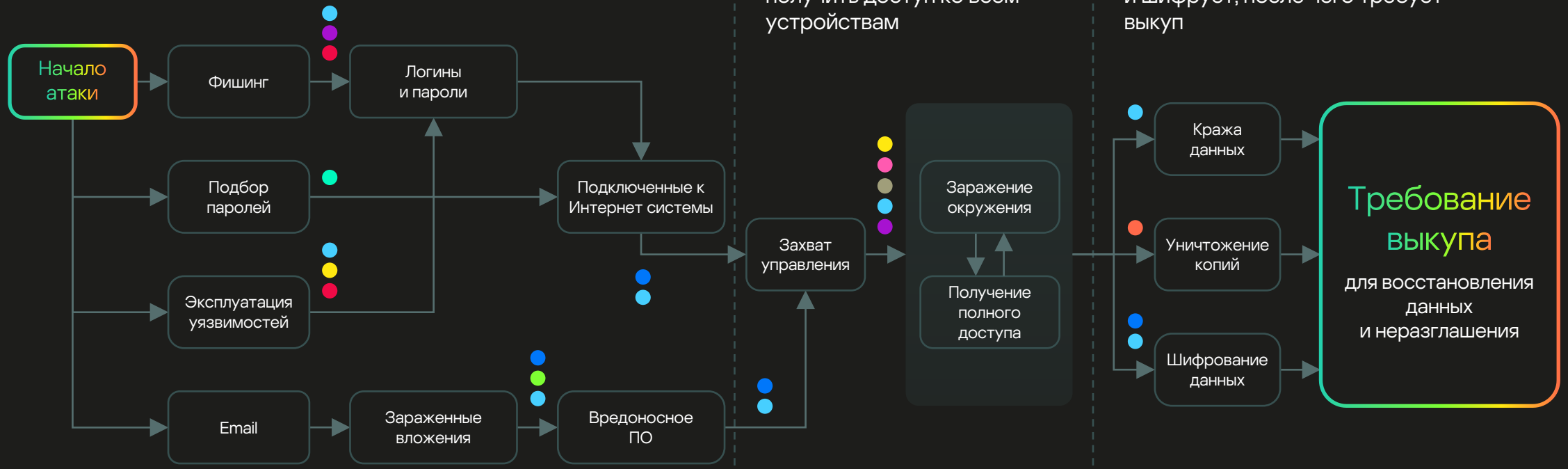
Злоумышленник ищет выход в сеть

Консолидация и подготовка

Злоумышленник пытается получить доступ ко всем устройствам

Воздействие на цель

Атакующий крадет данные и шифрует, после чего требует выкуп

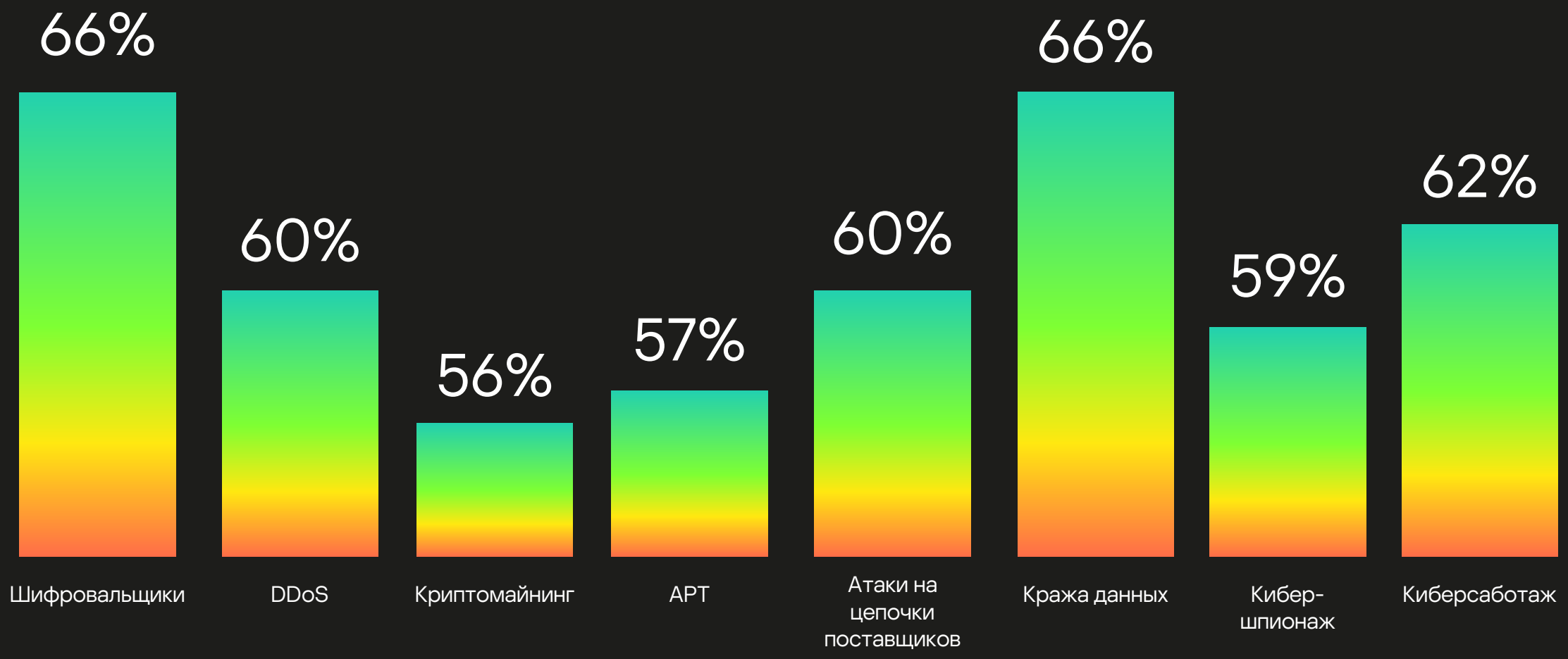


Критические контрмеры

CERT NZ Critical Controls for your business

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

Исследование: вероятность угроз. Мнение руководителей



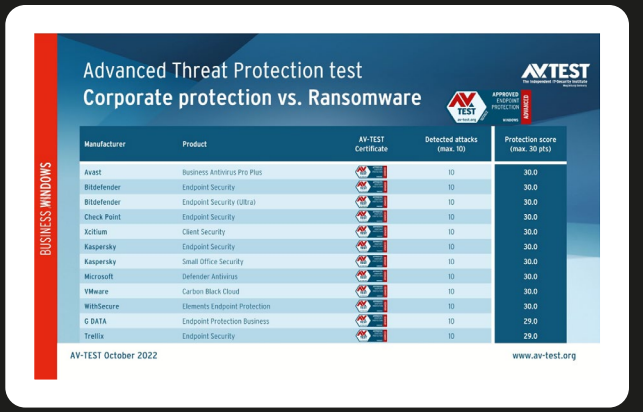
Kaspersky Survey, 2022

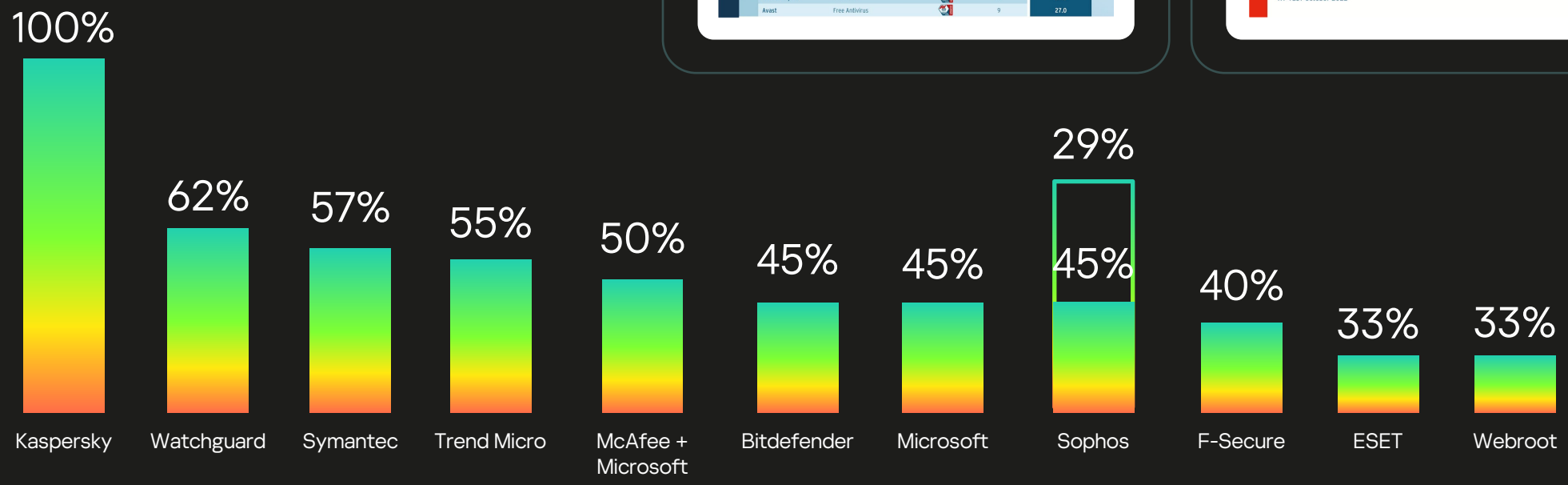
Лучшая защита от шифровальщиков

Атака полностью заблокирована

Атака частично заблокирована

Информация:
kas.pr/4mj2





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.

С 2018 года более 1,5 миллиона пользователей по всему миру смогли восстановить свои данные

80%

Массовые угрозы

19.9%

Целевые атаки

0.01%

APT

APT

Операция Триангуляция

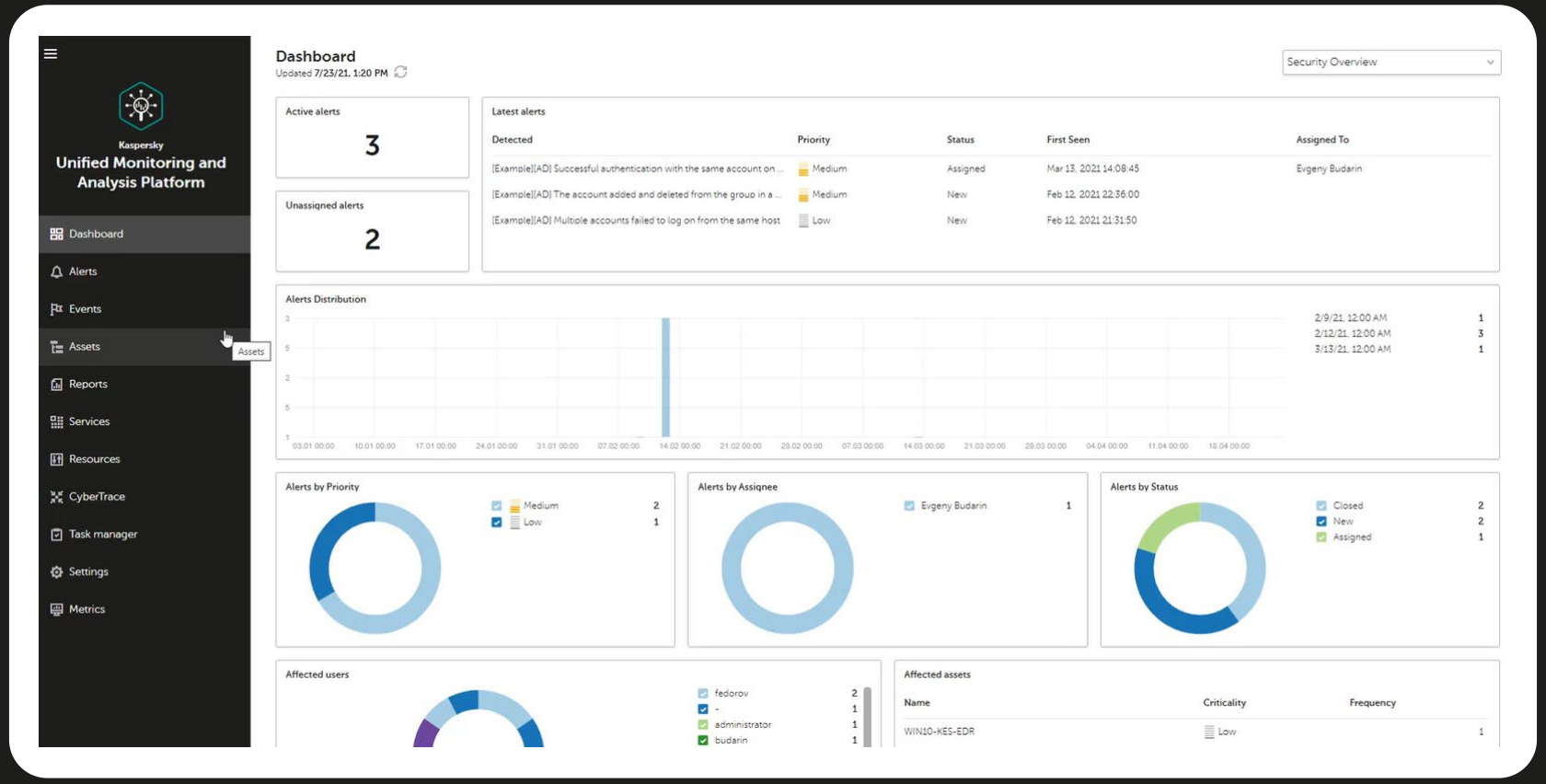
Операция Триангуляция: ранее неизвестная целевая атака на iOS-устройства

ОТЧЕТЫ О ЦЕЛЕВЫХ АТАКАХ (APT) 01 ИЮН 2023

5 мин. на чтение

Содержание

SIEM-система Kaspersky Unified Monitoring and Analysis Platform



Заражение «Триангуляцией»

1

Устройство получает невидимое сообщение iMessage с вредоносным вложением

2

Без взаимодействия с пользователем, эксплойт из сообщения вызывает выполнение вредоносного кода

3

Код соединяется с сервером управления и приводит к последовательной загрузке нескольких «ступеней» вредоносной программы

4

Злоумышленники получают полный контроль над устройством и доступ к данным

5

Все следы удаляются в процессе заражения

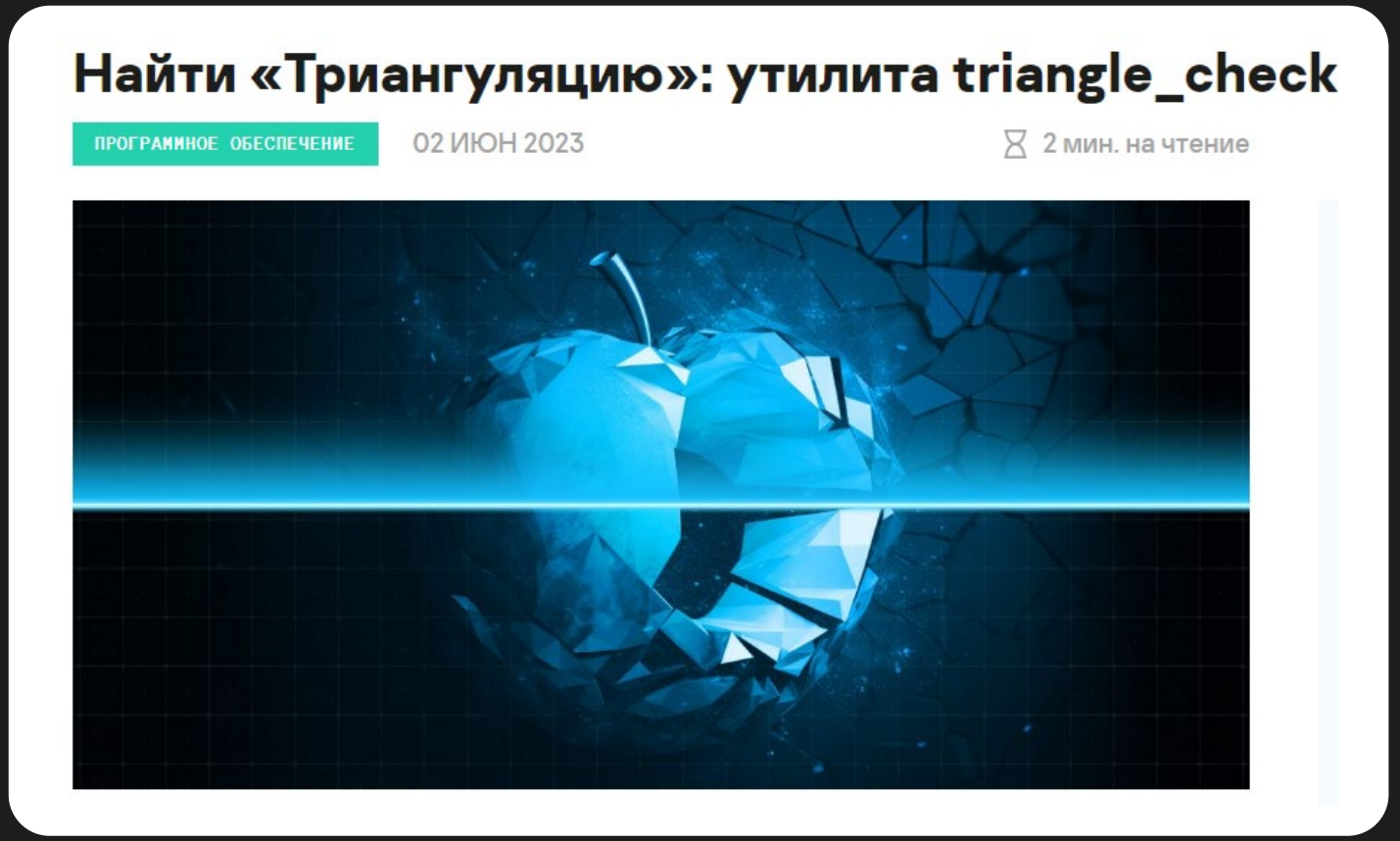
Защита от «Триангуляции»

Оперативное обновление iOS

Регулярная перезагрузка

Отключение iMessage

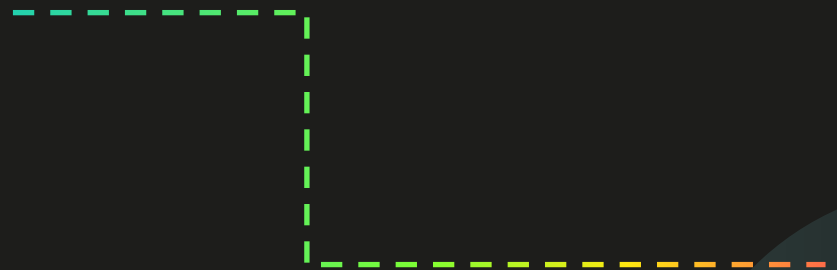
Проверить

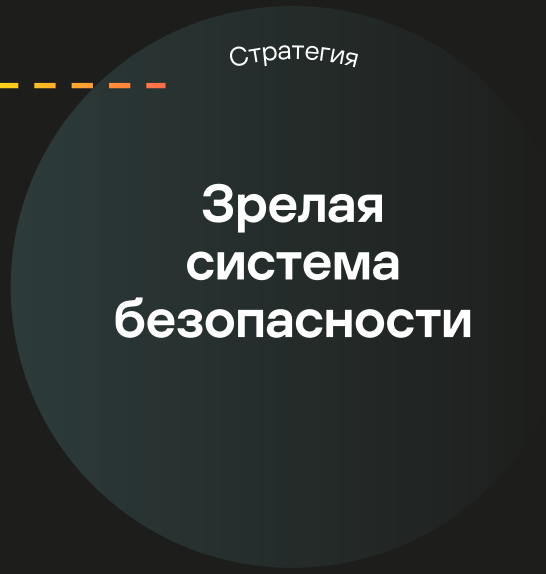


Что НЕ делать с APT?

Что необходимо компаниям в 2023 году?

Стратегия





encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Что необходимо компаниям в 2023 году?

Стратегия

Сотрудники

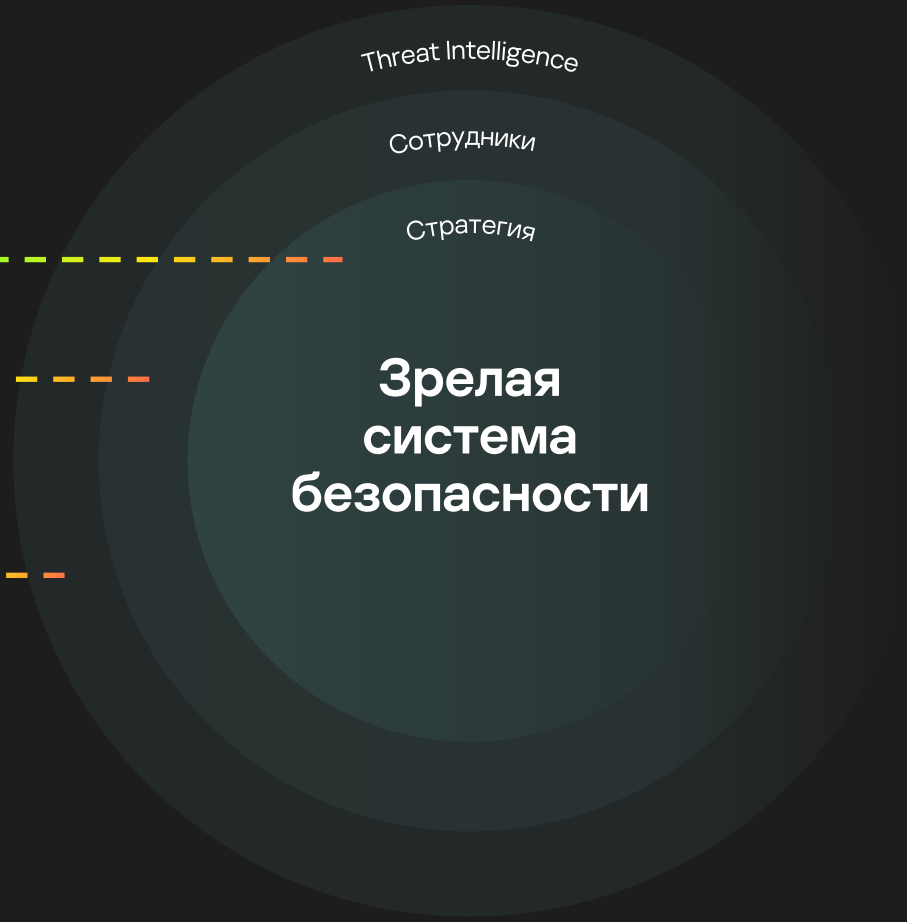
encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Что необходимо компаниям в 2023 году?

Стратегия

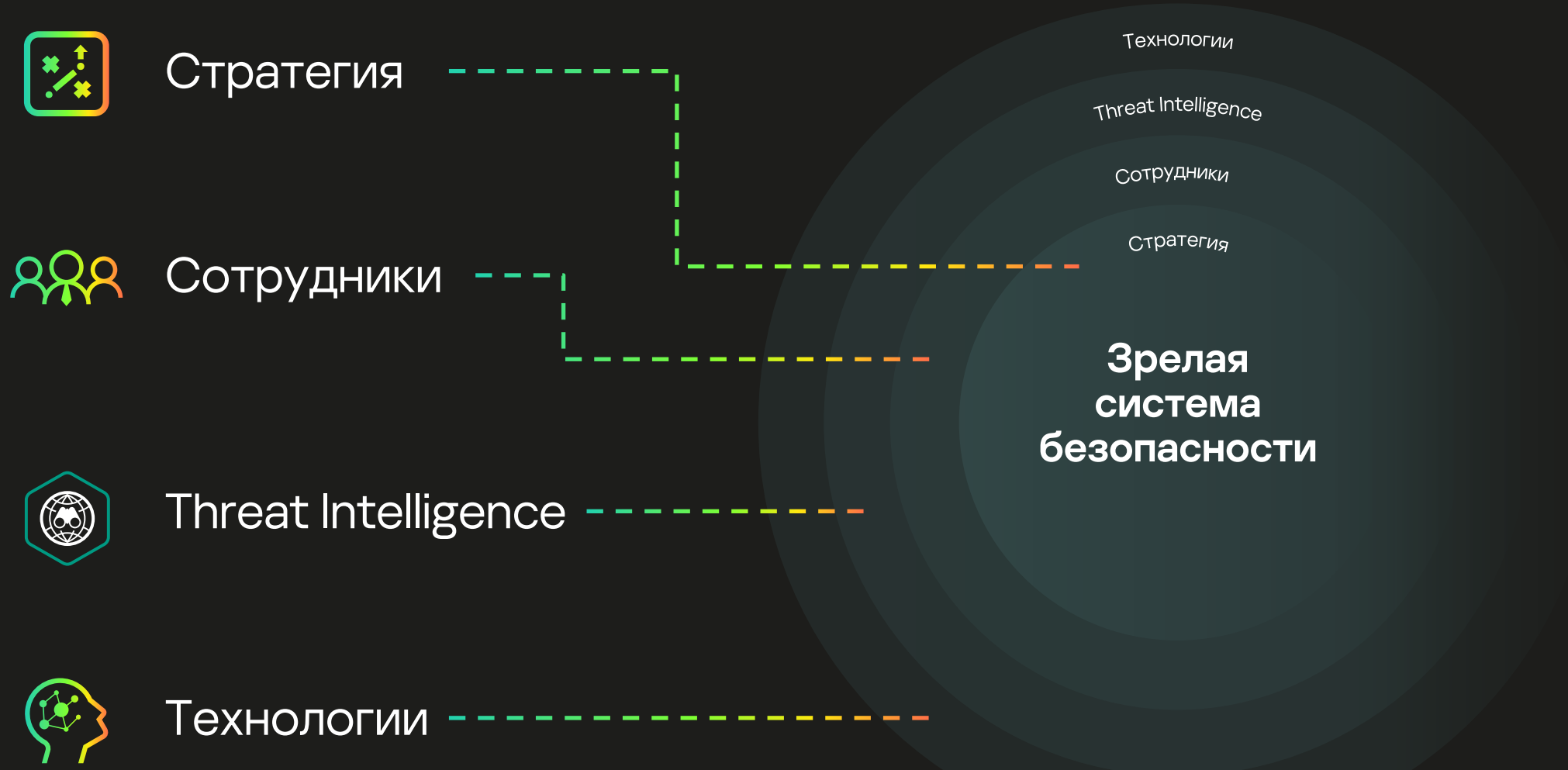
Сотрудники

Threat Intelligence



encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Что необходимо компаниям в 2023 году?



encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Спасибо!