



PT

# Актуальные киберугрозы

**III квартал 2020 года**

## Содержание

Резюме	3
Сводная статистика	4
Атаки с использованием вредоносных программ	8
Бум шифровальщиков	10
Промышленность остается под угрозой	14
Медицинские учреждения: вторая волна	16
В поисках вакцины	17
Атаки на периметр набирают обороты	17
Чего можно ожидать от шестилетнего трояна	19
Об исследовании	21

## Резюме

По итогам III квартала 2020 года мы отмечаем:

- Количество инцидентов в сравнении с прошлым периодом выросло всего на 2,7%. После резкого подъема в первом полугодии рост числа атак замедлился. Отдельно стоит отметить увеличение доли целевых атак с 63% до 70%.
- Произошел скачок числа атак на организации с использованием шифровальщиков. В прошлом квартале они составляли 39% всех атак с использованием вредоносного ПО, а в этом квартале их доля увеличилась до 51%. Таким образом, в каждой второй атаке с распространением вредоносного ПО были задействованы шифровальщики. Этим фактом объясняется и увеличение до 42% доли атак, в ходе которых злоумышленники преследовали финансовую выгоду.
- С начала этого года количество атак на промышленность держится на высоком уровне. По числу инцидентов эта отрасль занимает второе место. В основном атаки проводились АPT-группировками и операторами шифровальщиков (доля атак с использованием шифровальщиков составила 45%).
- Был зафиксирован очередной всплеск атак на медицинские учреждения. Половину всех инцидентов составляют атаки шифровальщиков, которые спекулируют данными пациентов, лишают больницы возможности работать, отрезая доступ к информационным системам, листам назначений и осмотров. Атакам подвергаются также исследовательские центры, которые занимаются разработкой вакцины от коронавируса.
- Доля атак с использованием методов социальной инженерии, в которых затрагивается тема COVID-19, сократилась с 16% во втором квартале до 4% в третьем. Мы связываем это, прежде всего, с тем, что люди постепенно привыкают к новой действительности и тема COVID-19 уже не производит такого сильного эффекта. К слову, если ранее в фишинговых рассылках предлагались средства защиты от вируса, то сейчас злоумышленники эксплуатируют интерес общества к вакцине.
- В сравнении с прошлым кварталом доля использования хакинга в качестве метода атак на компании увеличилась на 12 процентных пунктов и оставляет 30%. Мы связываем это с тем, что злоумышленники продолжают искать уязвимости в сервисах на периметре корпоративных систем. В связи с пандемией и переходом на удаленную работу многие компании вывели на периметр дополнительные сервисы, которые не всегда оказываются надежно защищены; таким образом, у преступников появилось больше возможностей для атак. Кроме того, системы, используемые для организации удаленного доступа, бывают подвержены известным уязвимостям, и мы видим, что эти уязвимости активно эксплуатируются.
- В июле вернулся в строй и уже получил статус самой актуальной угрозы троян Emotet. В будние дни рассылается более 500 тысяч писем, содержащих этот вредонос. Он крадет нужную ему информацию и передает доступ во внутреннюю сеть организации операторам программ-вымогателей и банковских троянов.

Для защиты от кибератак, прежде всего, мы советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. В свете новых тенденций грамотно выстроенный процесс управления уязвимостями становится не просто ответом на требования регулятора или на рекомендации отраслевого стандарта, а одной из приоритетных потребностей для корпоративной службы ИБ. Сейчас, с появлением средств автоматизированного сбора и анализа сведений об уязвимых сервисах, внедрить этот процесс в жизнь своей компании стало проще. Помимо эффективного процесса управления уязвимостями необходимо использовать современные средства защиты, включая WAF, средства анализа трафика, SIEM-системы. Для предотвращения атак, связанных с доставкой вредоносных программ по электронной почте, следует проверять вложения в песочнице — специальной виртуальной среде, предназначенной для поведенческого анализа файлов.

## Сводная статистика

В III квартале 2020 года мы выяснили, что взрывной рост активности злоумышленников, который наблюдался в первом полугодии на фоне начала пандемии COVID-19, начал замедляться. Однако число атак остается стабильно высоким, и тенденция к ежеквартальному увеличению количества инцидентов по-прежнему сохраняется. Так, в сравнении со II кварталом 2020 года количество атак выросло на 2,7%, а в сравнении с аналогичным периодом в 2019 году — на 54%.

### На 2,7% больше кибератак, чем во II квартале 2020 года

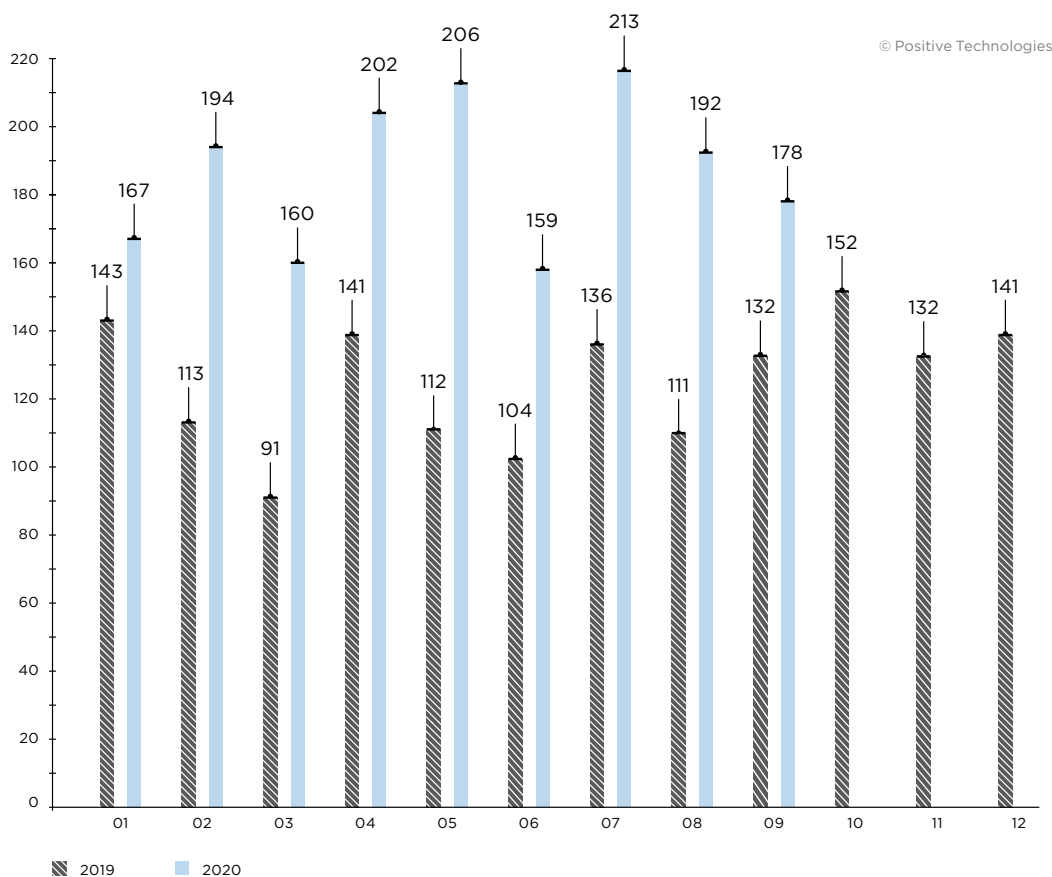


Рисунок 1. Количество инцидентов в 2019 и 2020 годах (по месяцам)

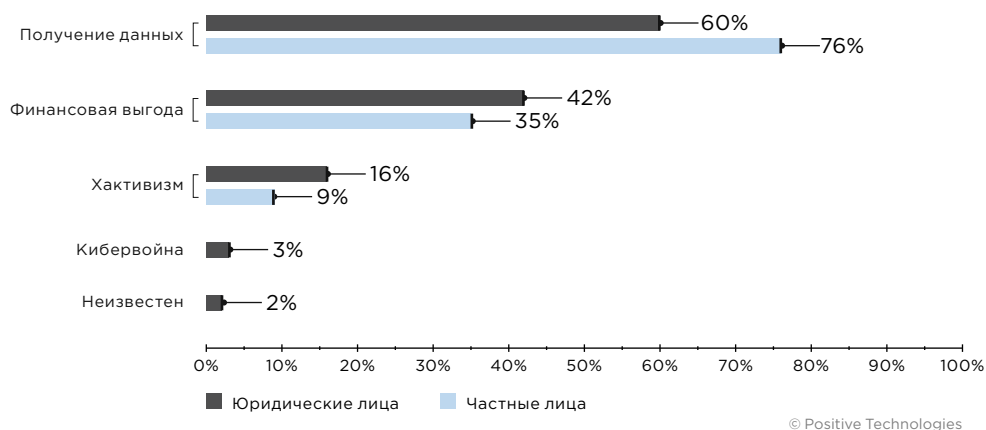


Рисунок 2. Мотивы злоумышленников (доля атак)

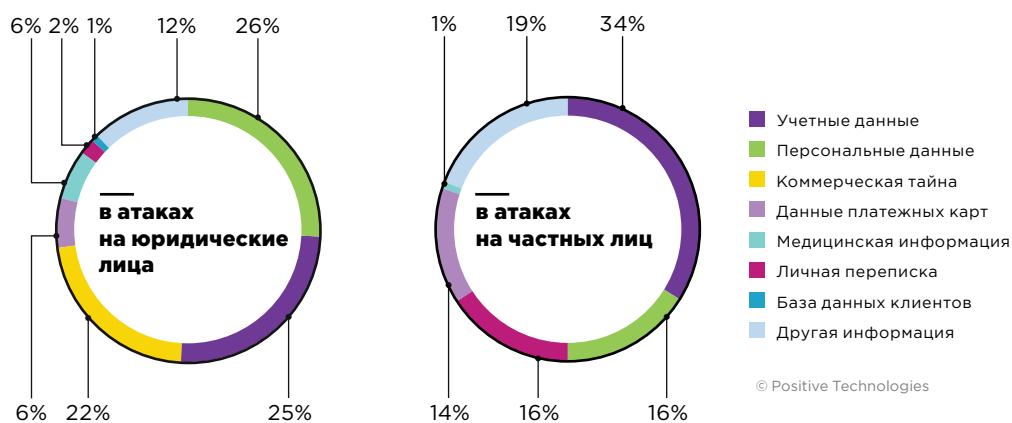


Рисунок 3. Типы украденных данных

**70% атак носят целенаправленный характер**

**18% атак направлены против частных лиц**

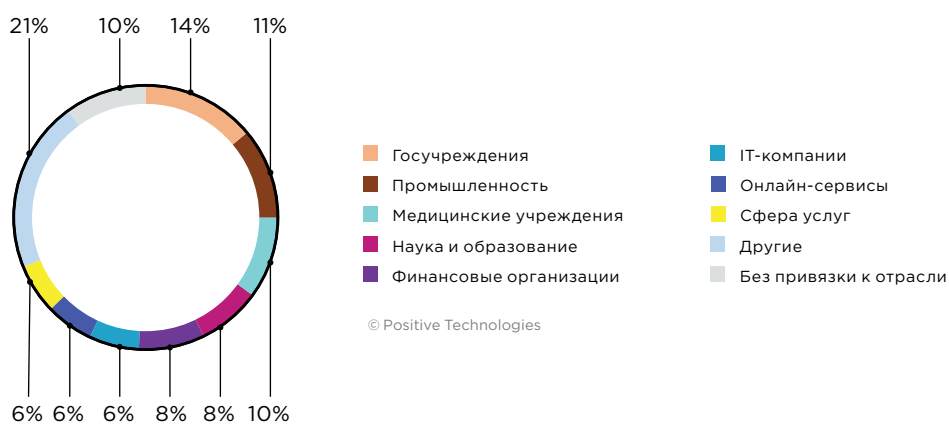


Рисунок 4. Категории жертв среди юридических лиц

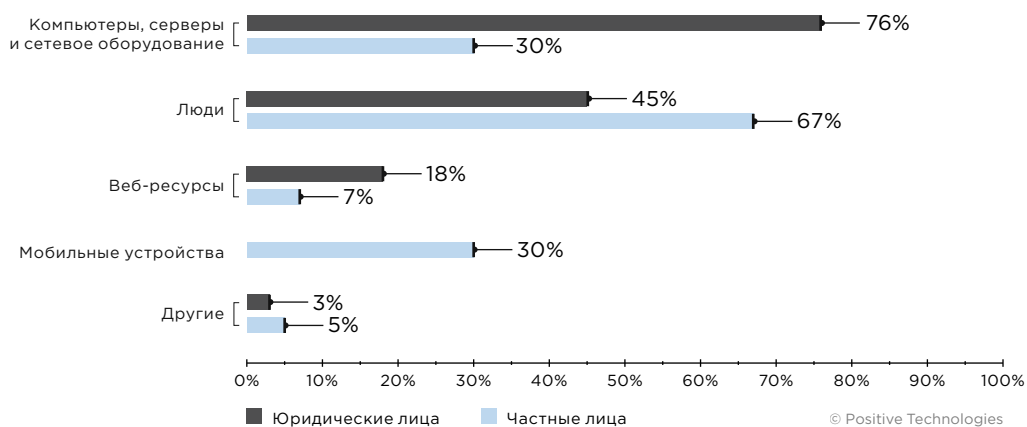


Рисунок 5. Объекты атак (доля атак)

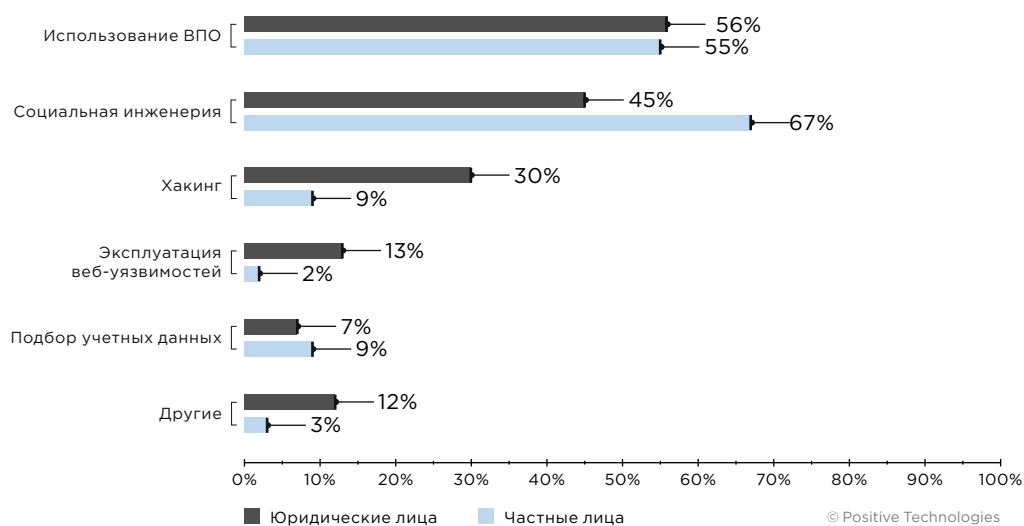
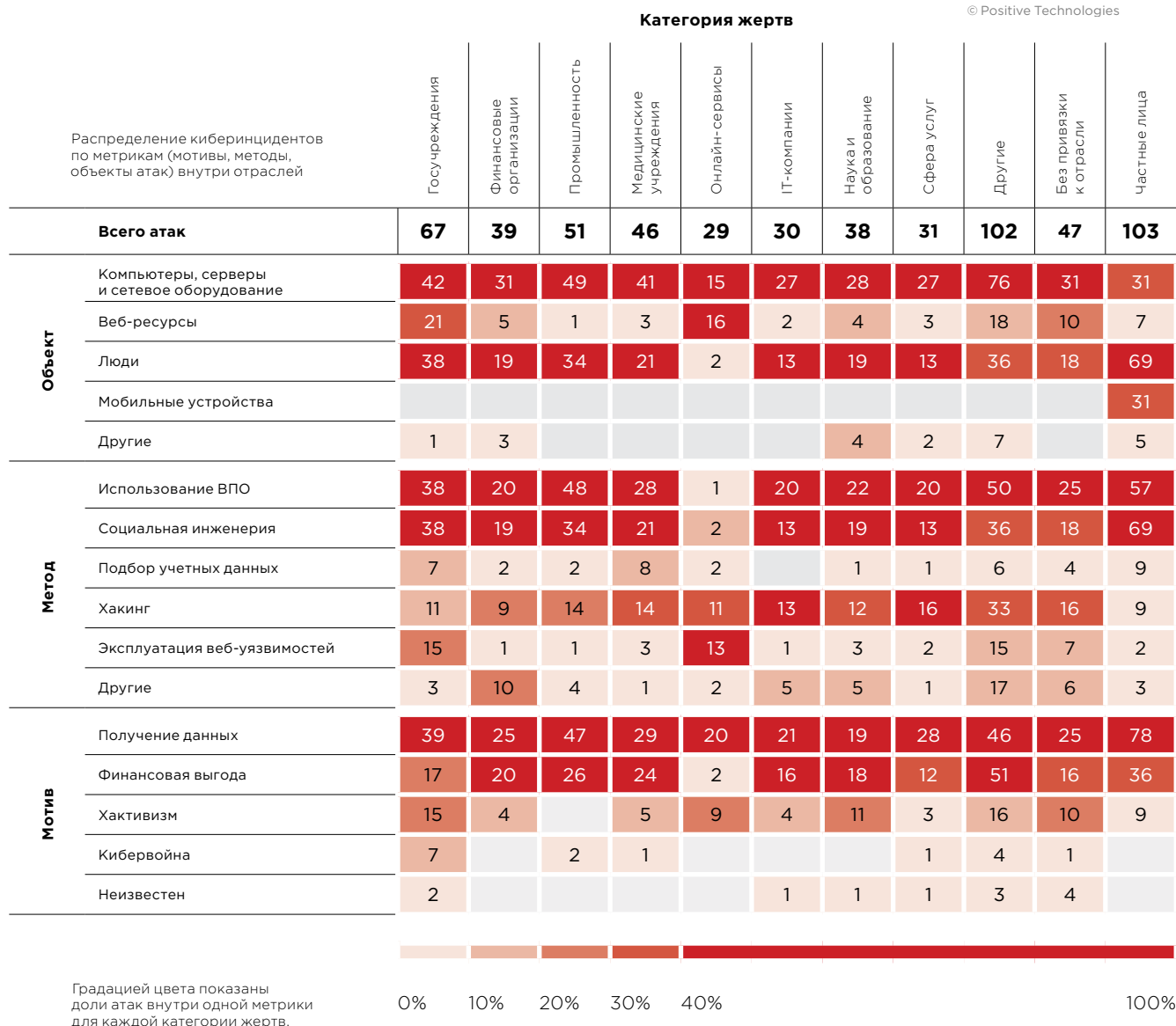
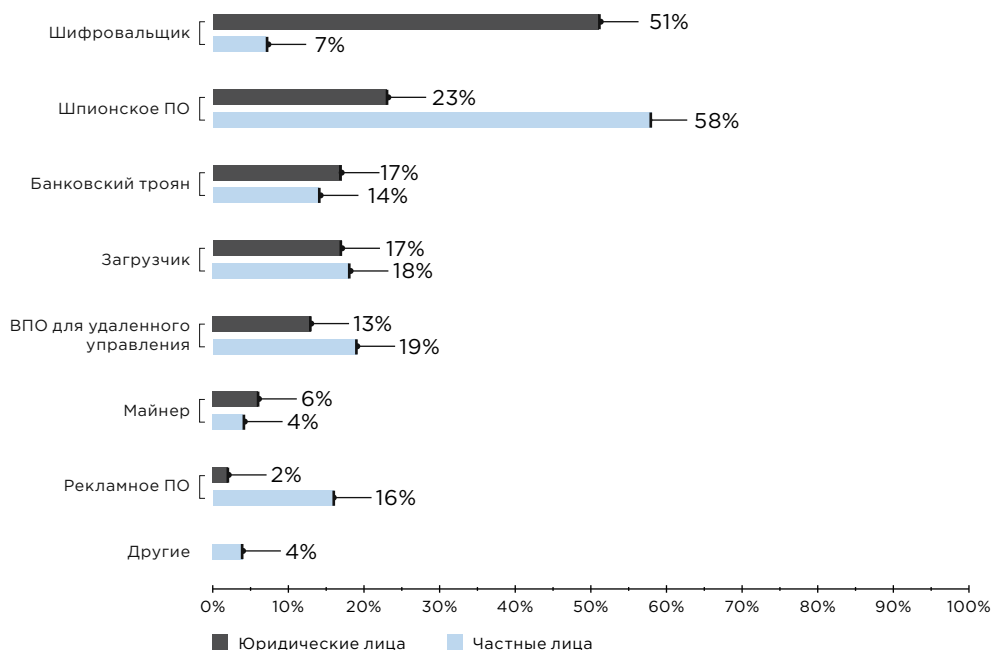


Рисунок 6. Методы атак (доля атак)



## Атаки с использованием вредоносных программ

В атаках, направленных против юридических лиц, неизменный тренд этого года — использование программ-вымогателей. Физических лиц, напротив, чаще атакуют программы-шпионы: в этом квартале их доля среди всех атак с использованием ВПО выросла на 18 п. п. и составляет 58%.



© Positive Technologies

Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)

Основным вектором проникновения во внутреннюю сеть компании и способом доставки вредоносного ПО по-прежнему является электронная почта. Однако с каждым кварталом мы наблюдаем тенденцию к увеличению числа атак, в которых вредоносное ПО распространяется путем эксплуатации уязвимостей на ресурсах сетевого периметра организаций. К примеру, как отмечают исследователи из компании Heimdal, операторы программы-вымогателя Netwalker до апреля 2020 года доставляли свой вредонос посредством фишинговых писем, а начиная с апреля изменили подход и теперь эксплуатируют уязвимости в необновленных VPN-решениях, подбирают пароли для удаленного доступа по протоколу RDP и ищут уязвимости в веб-приложениях.

Во многом этому тренду поспособствовала пандемия: компании в срочном порядке выводили на периметр сервисы, которые ранее были доступны только из локальной сети. В итоге периметр быстро менялся, не все уделяли достаточно внимания безопасности этих сервисов, и многие попросту не успевали обеспечить их надежную защиту. Большинство компаний все еще полностью или частично работают в удаленном режиме, поэтому вопросы инвентаризации доступных извне ресурсов и выстраивания эффективного процесса управления уязвимостями для них стоят особенно остро.



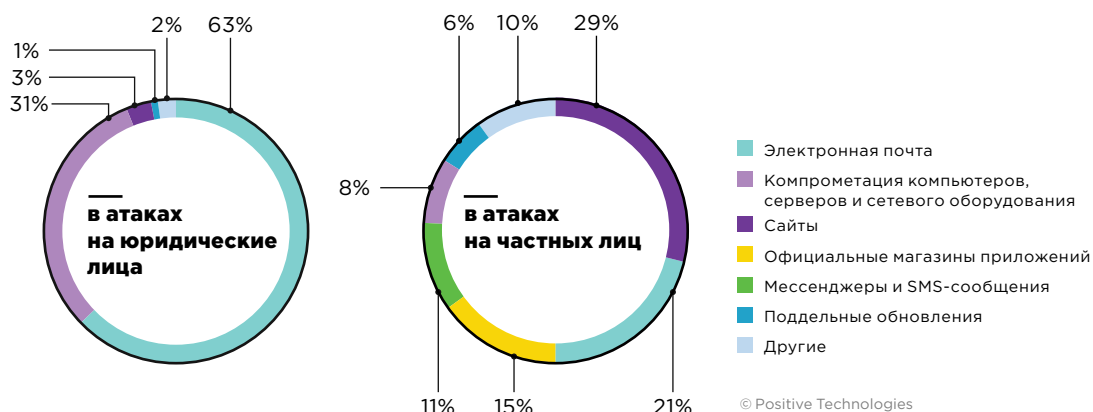


Рисунок 8. Способы распространения вредоносного ПО

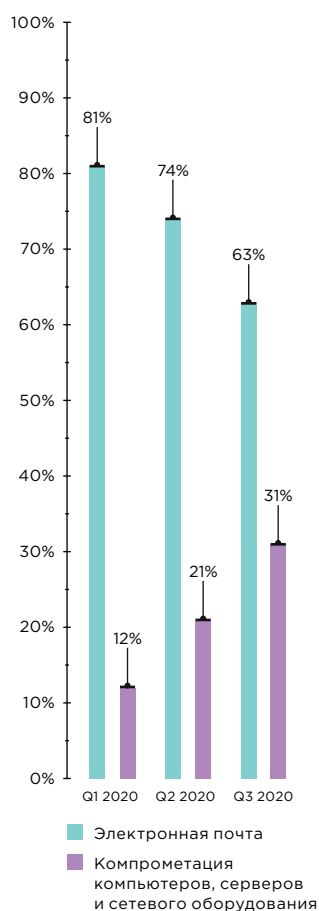


Рисунок 9. Основные способы распространения вредоносного ПО (доля атак на организации)

Также стоит отметить, что изобретательные злоумышленники придумывают новые способы сокрытия атак, чтобы как можно дольше оставаться незамеченными средствами защиты, в том числе и песочницами. В качестве наглядного примера рассмотрим августовский инцидент, связанный с атакой на международную архитектурную фирму. Целью злоумышленников была информация: снимки рабочего стола компьютера, пароли пользователей, файлы с определенными расширениями. Для проникновения во внутреннюю сеть компании хакеры создали специальный вредоносный плагин PhysXPluginMfx для Autodesk 3ds Max. Исследователи Bitdefender выявили занимательную особенность: вредонос проверяет, запущен ли диспетчер задач или Process Monitor, и в случае если какое-либо из этих приложений активно, он бездействует; это значительно затрудняет процесс детектирования.

Не менее интересный инцидент связан со старым шифровальщиком-вымогателем Zeppelin, который недавно вернулся в строй с новым загрузчиком. На его счету уже более 60 жертв. Распространяется это вредоносное ПО с помощью фишинговых писем, содержащих во вложении файл с расширением .doc. Открыв это вложение, пользователь тем самым запускает макросы, и далее приводится в действие механизм, устанавливающий загрузчик. Исследователи Juniper Threat Labs обнаружили, что Zeppelin научился скрываться от динамического анализа в песочнице: после того, как загрузчик выполнит свою роль — скачает исполняемый файл с шифровальщиком, вредоносная деятельность замирает на 26 секунд. Видимо, разработчики посчитали, что этого достаточно для завершения автоматизированной проверки в песочнице. По истечении этого времени происходит запуск самой программы-вымогателя Zeppelin.

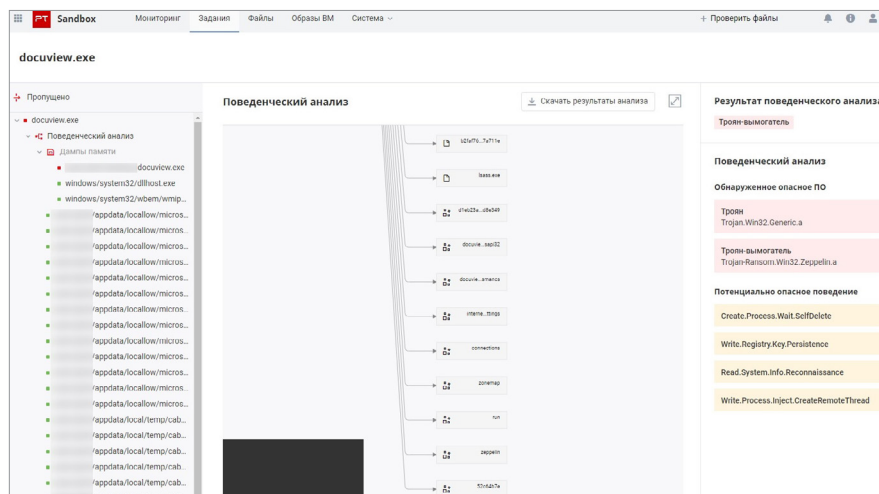


Рисунок 10. Процесс детектирования вредоносного ПО Zeppelin в песочнице

Более половины атак на частных лиц с использованием вредоносов были проведены с помощью шпионского ПО. Яркий пример — [инцидент с FakeSpy](#). Эта программа распространялась через фишинговые SMS-сообщения, которые содержали ссылку якобы от почтовой службы или службы доставки. После загрузки на мобильное устройство FakeSpy начинал собирать контакты, данные для входа в банковские приложения, отслеживать SMS-сообщения, а также отправлял подобные стартовые фишинговые сообщения всем контактам жертвы с целью дальнейшего распространения.

Также нельзя не отметить, что доля рекламного ВПО выросла в два раза, в прошлом квартале она составляла 8% от общего числа атак с использованием вредоносов, направленных на частных лиц. В качестве примера можно рассмотреть вредоносные программы из серии [RainbowMix](#), которые чаще всего маскируются под эмулятор Nintendo. Цель этих программ сводится к тому, чтобы показать рекламу якобы от легитимных приложений. Общее число загрузок RainbowMix превысило 14 миллионов, а максимальное количество показов рекламы составляло 15 миллионов за один день.

## Бум шифровальщиков

В III квартале произошел рекордный скачок числа атак с использованием программ-вымогателей; более половины атак с использованием вредоносного ПО составляют именно атаки шифровальщиков.

Операторы шифровальщиков все реже проводят массовые атаки, они целенаправленно выбирают крупные компании, которые в состоянии заплатить большой выкуп, или организации, для которых приостановка деятельности опасна, и наносят точечные удары. В этом квартале программы-вымогатели больше других атаковали промышленность и медицинские учреждения.

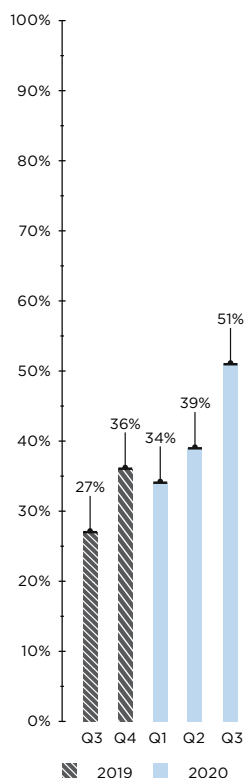


Рисунок 11. Атаки шифровальщиков (доля атак с использованием ВПО)

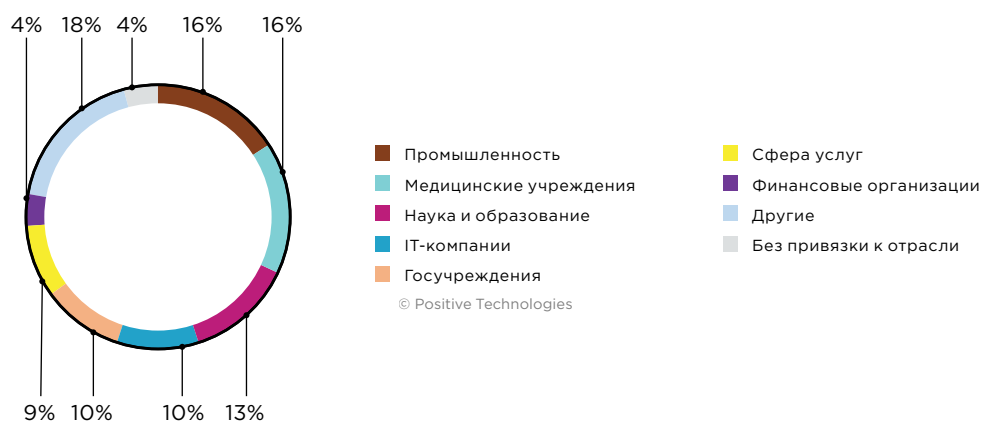


Рисунок 12. Атаки программ-вымогателей по отраслям

### **Топ-5 наиболее часто используемых программ-вымогателей в III квартале 2020 года**

1. Netwalker
2. REvil
3. Maze
4. DoppelPaymer
5. RansomEXX

В середине июля операторы программы-вымогателя REvil заразили внутреннюю сеть одного из крупнейших интернет-провайдеров Аргентины — Telecom Argentina. Хакерам удалось поразить более 18 000 рабочих станций. Выкуп, который они запросили за восстановление доступа, составил 7,5 млн долл. США. Еще один громкий случай в Аргентине произошел в конце августа и связан с миграционным агентством страны. Из-за атаки шифровальщика Netwalker была приостановлена работа на государственной границе. Чтобы восстановить доступ к инфраструктуре, операторы вредоносного ПО запросили 4 млн долл. США.

Также в августе была впервые замечена новая программа-вымогатель DarkSide. Операторы этого вредоносного ПО требуют выкуп от 200 тыс. до 2 млн долл. США и очень тщательно выбирают жертв, ориентируясь на собственное понимание, сможет ли та или иная компания заплатить выкуп. Они заявляют, что не будут атаковать медицинские, образовательные, государственные учреждения и некоммерческие организации. По словам специалистов из Advanced Intelligence, в процессе атаки вредоносное ПО избегает завершения определенных процессов, один из которых относится к приложению TeamViewer, что может указывать на то, что злоумышленники используют его для удаленного подключения к компьютерам. Одной из первых жертв нового вымогателя стал североамериканский застройщик Brookfield Residential: операторы DarkSide выкрали у него более 200 ГБ данных, включая коммерческую тайну, финансовую информацию, сведения о сотрудниках.

Операторы программы-вымогателя WastedLocker тоже подошли к выбору жертвы достаточно серьезно, атаковав в конце июля производителя GPS-навигационной техники и умных часов Garmin. Клиенты компании потеряли доступ к подключенным услугам и приложениям на несколько дней. Первоначально злоумышленники запросили за расшифровку данных 10 млн долл. США. Через четыре дня после атаки Garmin начала восстанавливать работоспособность своих сервисов. Предполагается, что компания все-таки пошла на сделку с хакерами, однако фактическая сумма выкупа неизвестна.

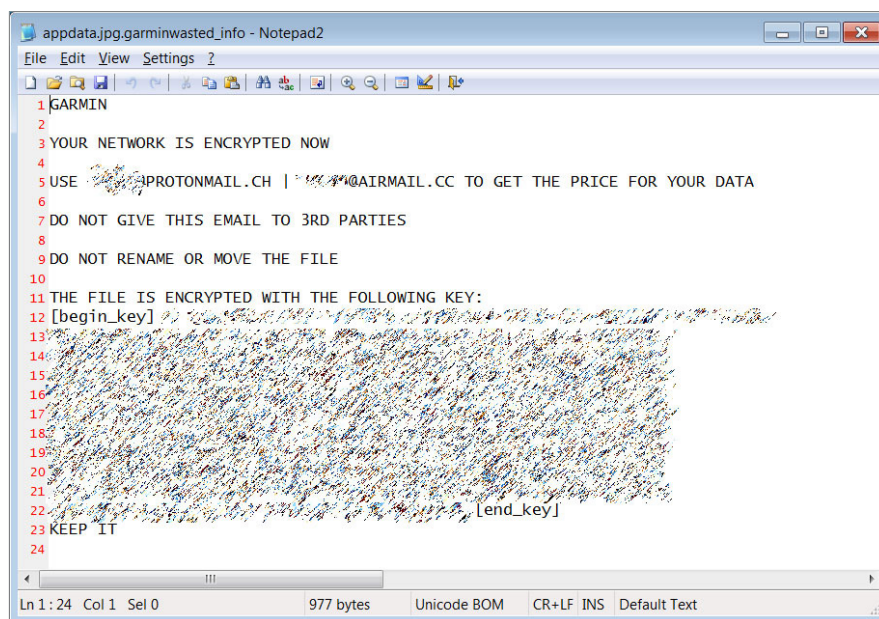


Рисунок 13. Записка с требованием выкупа, адресованная Garmin

В конце июля действия программы-вымогателя RansomEXX привели к нарушению работы сайта компании Konica Minolta, который был недоступен около недели. В это же время операторы Maze атаковали Canon — злоумышленники утверждали, что похитили 10 ТБ данных компании.

Не пощадили шифровальщики и китайские отделения французского судоходного гиганта CMA CGM. В конце квартала они были атакованы операторами программы-вымогателя Ragnar Locker. Около суток были недоступны система бронирования контейнеров, сайты и приложения компании.

В начале сентября от атаки шифровальщика Netwalker пострадала компания Equinix, которая предоставляет услуги обработки данных. Была похищена финансовая информация, данные аудитов и отчеты центра обработки данных, сведения о заработной плате и бухгалтерские документы компании. Запрашиваемый выкуп за программу-дешифратор и нераспространение украденных данных составил 4,5 млн долл. США. В своей записке хакеры также предупреждали, что если выкуп не заплатят быстро, то через некоторое время сумма будет удвоена. Представители Equinix не сообщают, как именно преступники проникли в сеть, однако исследователи из Advanced Intelligence обнаружили в даркнете объявления о продаже учетных данных для подключения к 74 серверам этой компании.

Ранее мы уже рассказывали о рынке преступных киберуслуг. В мире киберпреступности практикуется разделение обязанностей. Менее квалифицированные хакеры занимаются взломом сетей компаний, а затем продают доступ опытным злоумышленникам, которые смогут им грамотно воспользоваться. Пример с Equinix — это далеко не единственный случай даже среди крупных организаций; например, в сентябре в даркнете было размещено объявление о продаже доступа в корпоративную сеть компании — лидера мировой судостроительной промышленности. Стоимость составляет 10 биткойнов, по текущему курсу это более 100 тыс. долл. США.

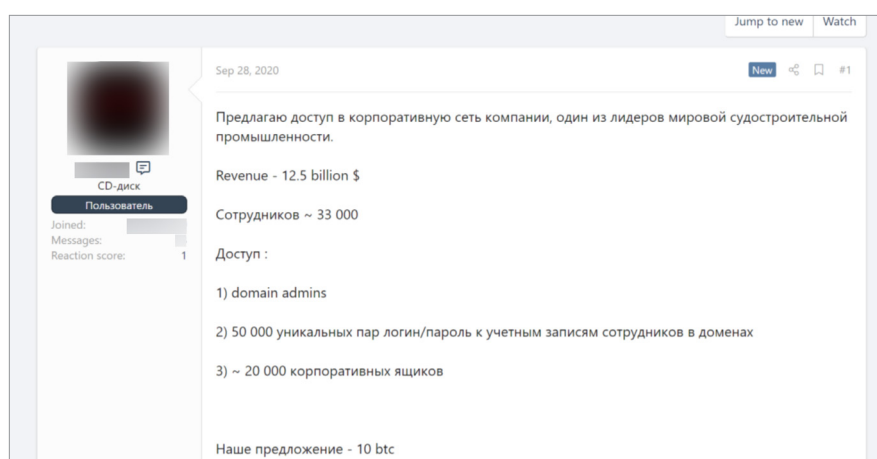


Рисунок 14. Продажа доступа к сети лидера судостроительной промышленности

Как мы уже отмечали, некоторые злоумышленники, прежде чем запустить шифровальщик, крадут информацию. Для публикации этого дорогостоящего контента в случае неуплаты выкупа они используют собственные сайты. В этом квартале такие площадки появились у SunCrypt, DarkSide и Conti.

Интересный факт: некоторые злоумышленники пытаются эксплуатировать авторитет выдающихся группировок. Например, операторы программы-вымогателя SunCrypt в конце августа заявили, что стали новым членом картеля Maze. Однако, похоже, что Maze были не в курсе этого сотрудничества, о чем говорится в их опровержении. По их мнению, операторы SunCrypt сделали это заявление в рамках PR-стратегии, для того чтобы сослаться на принадлежность к картелю и тем самым оказывать большее давление на жертв.

## Промышленность остается под угрозой

С начала этого года количество атак на промышленность держится на высоком уровне. В III квартале эту отрасль в основном атаковали АPT-группировки, в том числе RTM и TinyScouts, а также операторы шифровальщиков Nefilim, Maze, Netwalker, RansomEXX, Conti и DoppelPaymer. Доля атак с использованием шифровальщиков составила 45% от общего числа атак.

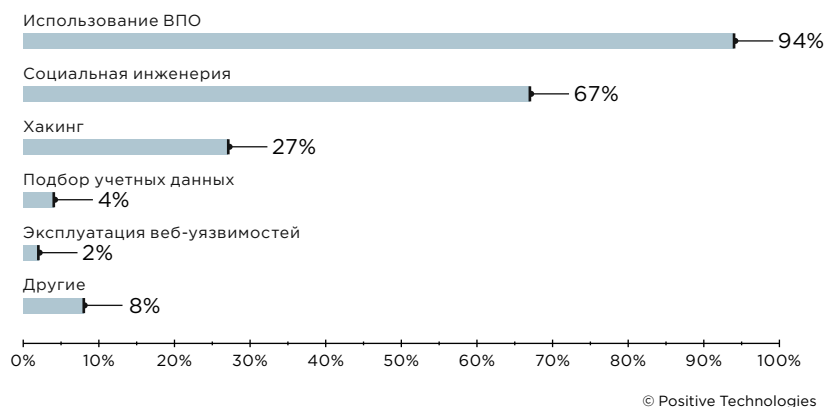


Рисунок 15. Методы атак (доля атак на промышленность)

Промышленность не стала исключением из тренда на эксплуатацию уязвимостей сетевого периметра, доля хакинга увеличилась более чем в два раза в сравнении с прошлым кварталом. Однако большая часть злоумышленников (67%) по старинке используют электронную почту в качестве основного способа проникновения. К примеру, так делает новая группировка TinyScouts, нацеленная, среди прочего, на энергетические компании. На первом этапе атаки злоумышленники рассылали сотрудникам различных организаций фишинговые письма — либо на тему COVID-19, либо составленные под конкретную жертву. В июльской кампании к письму прикреплялся файл с расширением .lnk, и когда пользователь открывал его, запускалась утилита mshta.exe. С ее помощью для пользователя открывался файл-заглушка, а для злоумышленников отработывал скрипт, проверяющий наличие TeamViewer, RDP-сессий и факт входа в домен. Далее следовала вариативная часть: если компания оказывалась интересной злоумышленникам, запускалась шпионская программа, собирающая все необходимые им данные, в противном случае начинал свою работу шифровальщик. Заметим, что схожим образом — с использованием файла с расширением .lnk и последующим запуском утилиты mshta.exe — атакует госучреждения АPT-группировка Gamaredon, активность которой специалисты PT Expert Security Center наблюдают на протяжении нескольких кварталов.

Методами социальной инженерии для доставки своего вредоносного ПО пользуется и АPT-группировка RTM. За этот квартал специалисты PT ESC обнаружили 34 случая фишинговых рассылок от этой группы.

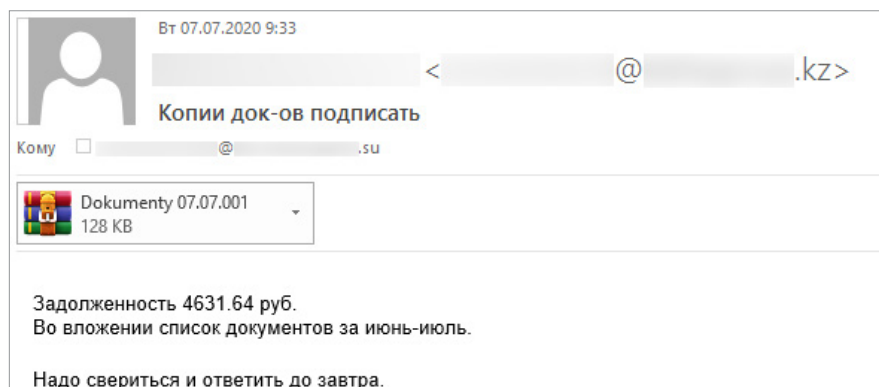


Рисунок 16. Письмо с вредоносным архивом от APT-группировки RTM

Каждая пятая атака в этом квартале была совершена с использованием программ-шпионов или вредоносных для удаленного управления. Злоумышленники прежде всего нацелены на кражу конфиденциальных сведений.

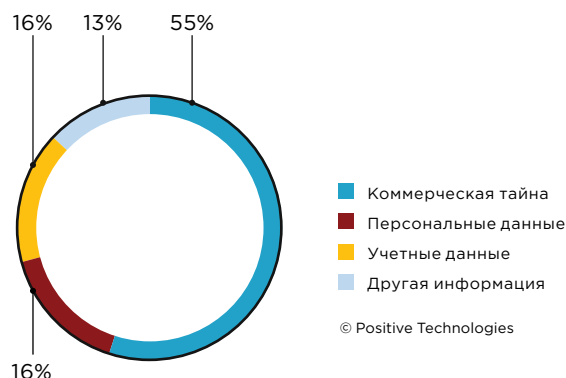


Рисунок 17. Данные, украденные в ходе атак на промышленность

Активность программы-вымогателя Netwalker не обошла стороной и сферу промышленности. Седьмого сентября был атакован единственный поставщик электроэнергии в пакистанском городе Карачи — K-Electric. В результате была нарушена работа онлайн-биллинга и других сервисов компании. За восстановление доступа операторы Netwalker требовали 3,9 млн долл. США, а в случае неуплаты в течение семи дней грозились поднять выкуп до 7,7 млн долл. США.

Операторы программы-вымогателя Maze провели успешную атаку на Hoa Sen Group — крупнейшего производителя стальных листов во Вьетнаме. В ходе этой атаки были похищены персональные данные сотрудников, внутренняя переписка и другая конфиденциальная информация. На данный момент в сеть выложено 1,64 ГБ файлов, что составляет 5% от общего объема украденных данных. От рук тех же злоумышленников пострадал и крупный поставщик оперативной и флеш-памяти, компания SK hynix. В результате этой атаки было похищено 11 ГБ информации, в том числе конфиденциальные соглашения с Apple о поставке флеш-памяти NAND.

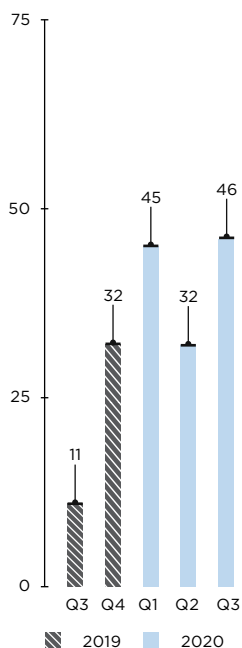


Рисунок 18. Число атак на медицинские учреждения

## Медицинские учреждения: вторая волна

Начиная с февраля 2020 года мы наблюдаем напряженную эпидемиологическую обстановку во всем мире. Больше всего ее прочувствовали медицинские учреждения, ведь колоссальная нагрузка на них практически не снижалась. Злоумышленники пользуются эпидемией, и в III квартале этого года был зафиксирован очередной всплеск количества атак, направленных на лечебные учреждения.

Половина атак на медучреждения были совершены операторами программ-вымогателей, и последствия этих атак имели значительные масштабы. Так, в конце сентября сеть больниц Universal Health Services в США была атакована программой-вымогателем Ryuk. Сотрудники больниц не могли получить доступ к результатам анализов пациентов и ранее сделанным назначениям, получить данные с диагностических приборов и оказать пациентам медицинскую помощь, поскольку компьютеры были выключены, а все необходимые данные хранились в электронном виде и оказались зашифрованы в результате атаки.

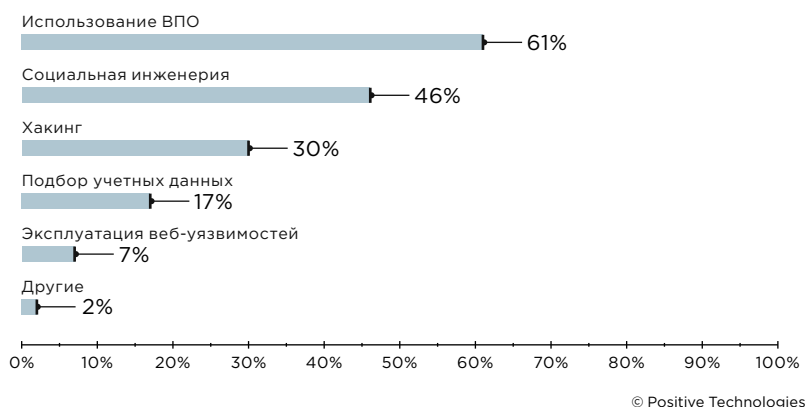


Рисунок 19. Методы атак (доля атак на медицинские учреждения)

Продолжает развиваться ранее наметившаяся тенденция к публикации украденной в ходе атак информации. В августе операторы программы-вымогателя REvil атаковали сеть больниц Valley Health в США, украв, а затем зашифровав всю информацию во внутренней сети. Чтобы доказать, что атака завершилась успехом, они выложили в сеть часть украденной информации, в том числе персональные данные пациентов, листы назначений и записи осмотров. В сентябре шифровальщик SunCrypt совершил атаку на Университетскую больницу Нью-Джерси. Были украдены 240 ГБ информации, включая данные о пациентах. После того как на сайте оператора программы-вымогателя появились 48 тыс. документов, принадлежащих больнице, представитель больницы связался со злоумышленниками, чтобы остановить публикации. В ходе переговоров сумма выкупа была снижена с 1,7 млн долл. США до 670 тыс. долл. США, и больница этот выкуп заплатила.

Некоторые хакеры используют официальные веб-ресурсы медицинских учреждений в качестве площадок для размещения своего контента. К примеру, злоумышленники воспользовались уязвимостями в платформах CMS сайтов Национальных институтов здравоохранения США и Национального института онкологии и разместили там статьи, посвященные взлому аккаунтов в популярных соцсетях. В этих статьях они предлагали воспользоваться якобы инструментом для взлома, за который требовалось заплатить: таким образом злоумышленники получали доступ к данным платежных карт и денежные средства на свой счет.



## В поисках вакцины

Под ударом оказались не только медицинские учреждения. Атакам подвергаются и исследовательские центры, которые занимаются разработкой вакцины от COVID-19. Например, в сентябре этого года были атакованы испанские исследовательские центры. Основной целью злоумышленников была информация о последних наработках и результатах апробации.

Тема COVID-19 эксплуатируется злоумышленниками и в атаках на физических лиц. Если в прошлом квартале в своих фишинговых рассылках злоумышленники предлагали средства защиты или дополнительную информацию о вирусе, то сейчас они чаще спекулируют на теме вакцины. Например, в одной из рассылок, направленной жителям Великобритании, говорилось о том, что работа по созданию местной вакцины движется медленно, и предлагалось заказать готовую вакцину на сайте канадской аптечной сети. Стоит ли говорить, что ссылка вела на поддельный сайт, где пользователи оплачивали воздух?

Впрочем, количество фишинговых рассылок о COVID-19 быстро идет на спад. Доля атак с использованием методов социальной инженерии, в которых затрагивается тема пандемии, сократилась с 16% во втором квартале до 4% в третьем.

## Атаки на периметр набирают обороты

В настоящее время меняется подход к выбору способов проникновения во внутреннюю сеть организаций. Практически во всех отраслях наблюдается рост доли хакинга относительно других способов проникновения, что вполне объяснимо на фоне повсеместного перехода на удаленный режим работы и быстрого изменения состава сервисов на сетевом периметре многих компаний.

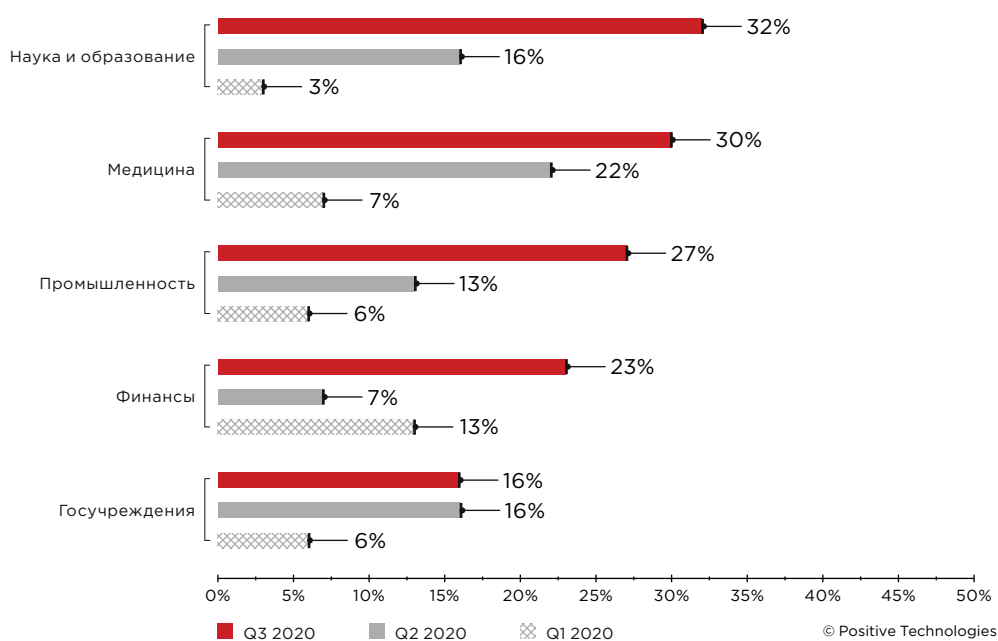


Рисунок 20. Доля хакинга среди методов атак (наиболее часто атакуемые отрасли)

### **Наиболее часто эксплуатируемые уязвимости в III квартале 2020 года**

- CVE-2019-19781 (Citrix NetScaler ADC, Gateway и SD-WAN)
- CVE-2019-2725 (Oracle WebLogic Server)
- CVE-2019-11510 (Pulse Secure VPN)
- CVE-2020-5902 (F5 BIG-IP)

Все чаще в новостях мелькают названия уязвимостей в контексте вектора атаки. Так, например, в августе злоумышленники, воспользовавшись уязвимостью CVE-2019-19781, которая позволяет выполнить произвольный код, атаковали итальянского производителя очков и средств для защиты глаз Luxottica. За пару недель до этого был атакован оператор круизных линий Carnival Corporation. Исследователи из Bad Packets проанализировали инцидент и выявили на сетевом периметре компании несколько уязвимых устройств. Для проникновения в локальную сеть злоумышленники могли воспользоваться, например, уязвимостью CVE-2019-19781 в Citrix ADC или CVE-2020-2021 в межсетевом экране Palo Alto Networks.

В конце июня — начале июля произошел инцидент, в котором эксплуатировалась уязвимость CVE-2019-11510, позволяющая читать произвольные файлы на сервере. Хакер просканировал все адресное пространство IPv4 в интернете для серверов Pulse Secure VPN, а затем использовал эксплойт для CVE-2019-11510. В итоге он получил более 900 пар логинов и паролей, а также IP-адреса для доступа к веб-серверам — и предоставил их в свободном доступе всем желающим. Исследователь Bank Security проанализировал данные, предоставленные злоумышленником, и пришел к выводу, что на всех включенных в список серверах Pulse Secure VPN действительно была установлена версия ПО, уязвимая для CVE-2019-11510.

Исследователи компании Panda Security установили, что уязвимость CVE-2019-2725, позволяющую удаленно выполнить произвольный код, часто используют в своих атаках операторы программы-вымогателя REvil. В июле этого года REvil провели несколько атак на испанскую железнодорожную компанию Adif. Было похищено 800 ГБ данных — коммерческая тайна, бухгалтерские документы, персональные данные и электронная переписка.

Активы / Состояние на сейчас

**8.8 Перехват контроля | CVE-2019-2725**

Изменить статус | Отметить как важную | Изменить метки

Обнаружена

### Основная информация

Опасность ■ Высокий уровень

Эксплойт ■ Есть

Удаленная эксплуатация ■ Да

Статус Новая

Устранение ■ Нет политики

Актив ■

### Описание

Уязвимость в Oracle Fusion Middleware в компоненте Oracle WebLogic Server (в подкомпоненте Web Services) позволяет злоумышленникам, не прошедшим аутентификацию и имеющим доступ к сети по HTTP, скомпрометировать Oracle WebLogic Server и получить контроль над ним.

### Как исправить

Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:  
<http://www.oracle.com/>

### Метрики CVSS v3

Общая оценка 8.8

Базовый вектор 9.8 — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Временной вектор 8.8 — EP:RLO/RC:C

### Дополнительная информация

Идентификатор [CVE-2019-2725](#)

Пентест-проверка ■ Возможна

Уязвимое ПО ■ Oracle WebLogic Server

Способ обнаружения ■ Расчет

Найдена уязвимость в ПО Oracle WebLogic Server

ПО на узле

Класс ■ Software:Oracle.WebLogicServer

Название ■ Oracle WebLogic Server

Версия ■ 10.3.6.0 ∈ [ 10.3.6.0; 10.3.6.0 ]

[Свернуть подробности](#)

### Активы с такими же уязвимостями

Значимость	Активы
<span style="color: red;">■</span> Высокая	0
<span style="color: orange;">■</span> Средняя	0
<span style="color: blue;">■</span> Низкая	0
<span style="color: gray;">■</span> Не определена	1
<b>Всего</b>	<b>1</b>

### Группы с такими же уязвимостями

Группа	Активы
<span style="color: blue;">■</span>	1

### Идентификаторы в базах данных

Идентификатор	Активы
<a href="#">CVE-2019-2725</a>	1
<a href="#">BDU-2019-01748</a>	1
MPBID: MPBID-191955	1

Рисунок 21. Обнаружение CVE-2019-2725 с помощью MaxPatrol VM

Некоторые уязвимости способствуют созданию бот-сетей. Например, исследователи компании Trend Micro обнаружили новую версию ботнета Mirai IoT, который нацелен, среди прочего, на эксплуатацию уязвимости CVE-2020-10173 (она связана с внедрением команд в маршрутизаторах Comtrend). Эксперты полагают, что эту брешь будут использовать и другие ботнеты — для проведения DDoS-атак.

## Чего можно ожидать от шестилетнего трояна

После непродолжительного отсутствия с февраля по июль была снова замечена активность трояна Emotet. Распространяется он посредством фишинговых писем и обладает функциями загрузчика, что позволяет осуществлять доставку других вредоносных программ. В начале новой волны атак Emotet распространял шпиона Trickbot, который после сбора информации открывал доступ для шифровальщиков Ryuk и Conti. Однако в скором времени ситуация изменилась, о чем сообщили исследователи, отслеживающие деятельность Emotet: теперь злоумышленники устанавливают на компьютеры жертв банковский троян QakBot (QBot).

Эксперты CISA считают, что Emotet — одна из самых актуальных угроз. Сперва зловердная волна затрагивала только организации в США, однако в августе и сентябре появились предупреждения об атаках во Франции, Японии, Новой Зеландии, Канаде, Италии и Голландии.

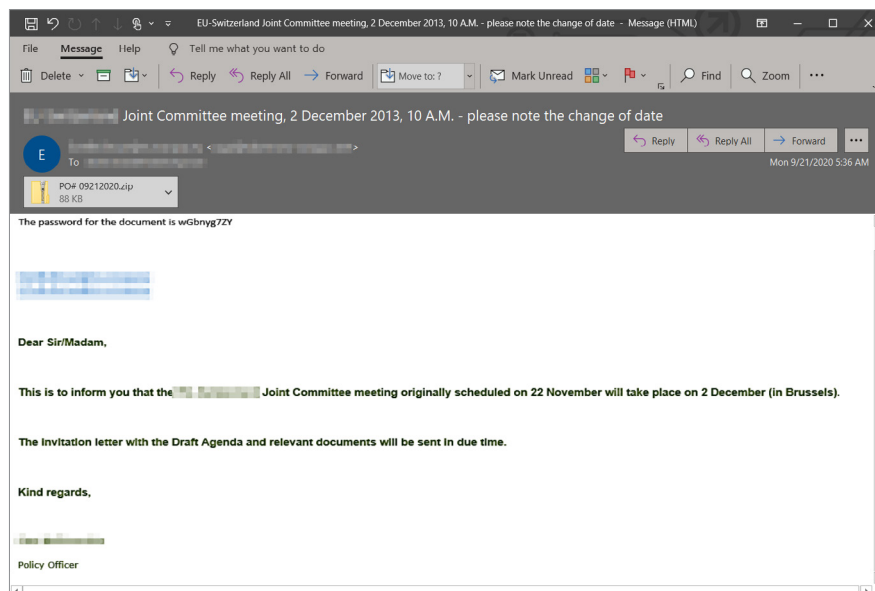


Рисунок 22. Пример фишингового письма от Emotet в цепочке писем

В начале атаки пользователю направляется письмо с вредоносным вложением. После открытия приложенного файла и активации макросов начинается загрузка исполняемого файла Emotet. Как только установка завершается, компьютер становится частью ботнета и приступает к отправке писем контактам жертвы. Для последующего распространения хакеры используют существующие цепочки писем в электронной почте на зараженном компьютере: они отвечают на письма из цепочки, в этом случае получатели полностью доверяют отправителю и открывают прикрепленный вредоносный файл.

Компания Microsoft в своем предупреждении отмечает, что Emotet ежедневно, за исключением выходных, рассылает более 500 000 писем. Для того чтобы пройти шлюзы безопасности электронной почты, злоумышленники прикрепляют во вложении защищенный паролем архив.

## Об исследовании

Данный отчет содержит информацию об актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах многочисленных расследований, а также на данных авторитетных источников.

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, в связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Наше исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены [в глоссарии на сайте Positive Technologies](#).

---

### О компании

[ptsecurity.com](https://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/](https://facebook.com/PositiveTechnologies)  
[PositiveTechnologies](https://facebook.com/PHDays)  
[facebook.com/PHDays](https://facebook.com/PHDays)

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте [ptsecurity.com](https://ptsecurity.com).